Government of Canada Gouvernement du Canada

Blended Horizontal Engagement of Information Technology (IT) Security: Part 2 – Targeted Internal Audit of IT Security Self-Assessments Completed by Small Departments

From Treasury Board of Canada Secretariat

April 2022
Office of the Comptroller General, Internal Audit Sector

Notice to readers

This report contains either personal or confidential information, or information related to security, which has been redacted in accordance with the Access to Information Act.

On this page

General overview

▼ In this section

Background – Blended Horizontal Engagement of IT Security

In 2019, the Office of the Comptroller General (OCG) launched a Blended Horizontal Engagement of Information Technology (IT) Security, incorporating a mix of both assurance and consulting activities, [1] to address a variety of IT security risks identified within the Government of Canada (GC). The engagement comprised the following parts:

Part 1

- Review of the IT security risk management process supporting the GC Digital Direction [2] (completed in fall 2020)

Part 2

- Mandatory IT security self-assessment in 36 small departments [3] (completed in fall 2019)
- **Focus of this report:** targeted internal audit of IT security self-assessments conducted for a risk-based sample of three small departments

Part 3

- Review of the effectiveness of user awareness and training and incident detection with three simulations (completed in fall 2020):
- simulation 1: spear phishing
- simulation 2: incident endpoint detection
- simulation 3: incident detection in the cloud

About the self-assessment – Part 2

With Part 2 of this engagement, a self-assessment tool [4] was developed by the OCG to help small departments gauge their progress toward implementing key IT security controls and identify areas where improvements could be made. The areas assessed were:

- IT security governance
- Communications Security Establishment (CSE) Top 10 security actions [5]
- IT security training and awareness
- incident management

The 36 of 47 small departments [6] selected by the OCG were required to complete the IT security self-assessment tool. The OCG compiled the results.

In fall 2019, participating small departments were provided with individual tailored reports by the OCG that summarized their departmental self-assessment results, including a comparative analysis with their peer groups [7] and the trends observed across all small departments. In addition to enabling the sharing of good practices between small departments, the goal of these reports was to:

- help raise awareness in all participating small departments about the state of each department's key IT security controls
- provide insights into which areas departments should consider prioritizing for improvement

Appendix D provides a summary of the results observed across the small department community included in the self-assessment exercise.

Note: Although large departments were excluded from this exercise, the self-assessment tool was distributed to them for their information and internal use as deemed appropriate at their discretion.

About the audit – Part 2

▼ In this section

Purpose of this report

This report presents the key take-aways, recommendations and general advice that stem from the internal audit portion of Part 2 of the Blended Horizontal Engagement of IT Security.

The primary audience for this report constitutes the small departments selected for inclusion in the audit.

Small departments that were not included in this audit are encouraged to:

- assess the applicability of the recommendations and general advice section contained in this report in consideration of their own respective contexts
- develop their own management action plans and follow up on them internally, where appropriate

Audit objectives

1. Verify the accuracy of the IT security self-assessment results reported for a risk-based sample of small departments.
2. Provide insights on potential government-wide barriers and root causes for findings relating to key IT security areas.

Scope

A risk-based approach (see Appendix E) was used to select the following three small departments for inclusion in this internal audit:

- [Redacted]
- [Redacted]

- [Redacted]

Given this small sample size, audit results provide only a limited indication of the overall reliability of self-assessments completed by the 36 participating small departments. The results of this audit therefore cannot be used to extrapolate on the reliability of the entire population of self-assessment results provided by the 36 participating small departments.

In order to increase the depth of insights on potential government-wide barriers and root causes related to the audit findings, the following three small departments were also consulted as part of this internal audit (refer to Appendix E for details):

- [Redacted]
- [Redacted]
- [Redacted]

The audit examined practices in place as of May 31, 2020.

Exclusion

The audit did not include testing of the effectiveness of IT security controls.

Approach

The approach for this audit consisted of assessing the documentation provided by each of the three participating small departments to support their self-assessed ratings. Within each of these departments, follow-up interviews were also conducted with senior-level departmental representatives who had key IT security responsibilities.

Criteria for this audit comprised the 20 questions included in the self-assessment tool, with their corresponding predefined ratings scales. Each rating referred to a maturity level, and specific attributes were set out for each level (see Appendix B for the self-assessment tool questions and rating scales, including maturity level attributes).

The maturity levels are shown in Table 1.

Table 1: Maturity levels

Low maturity	Medium maturity	High maturity	Unknown maturity
Level 1	Level 2	Level 3	“?”

A question mark (“?”) was assigned if a department was unaware or unsure of its maturity level for any given question assessed (this was considered a situational awareness issue). It should also be noted that a question mark was counted as a zero in calculating average maturity presented in Figure 1.

Why is this important?

The federal government is entrusted with safeguarding a vast amount of personal and sensitive information in delivering its programs and services to Canadians, and it relies heavily on IT. Threat actors have been known to take advantage of the interconnectedness of technology by using compromised systems as a platform for attacking other network areas to inflict significant damage. It is therefore important for all departments, including small departments, to be aware of and strategically manage their IT security controls.

The intention of this audit was not to set target maturity levels for small departments; IT security controls need to be tailored commensurate with departmental risk environments. Rather, the audit was meant to:

- complement the self-assessments by helping to further refine awareness about the state of key IT security controls within the

participating small departments
- provide specific recommendations on which areas that small departments should consider as priorities for improvements

Notwithstanding the small sample size for this audit, variances observed between self-assessment results and audit results are an important consideration for all participating small departments (or any other departments using the OCG self-assessment tool) to interpret their own self-assessment results. For instance, the variances observed as part of this audit may help provide an indication of areas where a risk of significant overestimation of maturity levels by management is more likely.

Audit findings

▼ In this section

Finding

Small departments overestimated the maturity levels of their IT security to varying degrees.

Key take-aways

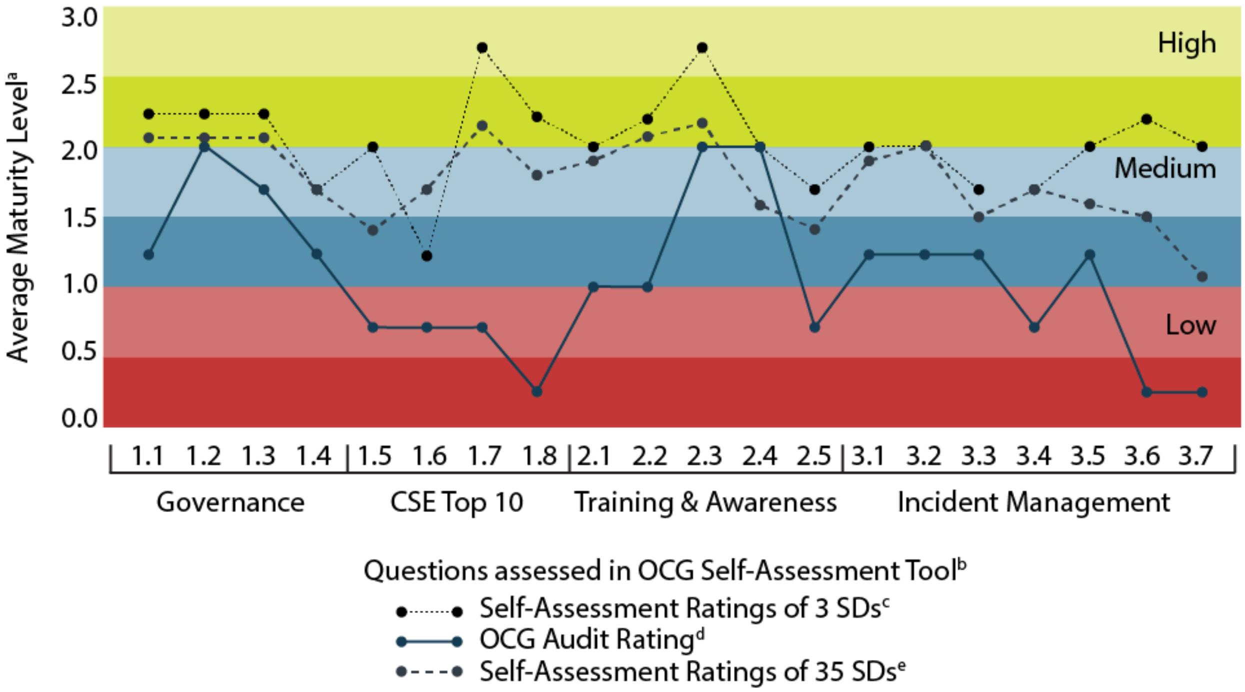
- The departments audited overestimated their IT security maturity to varying degrees in the vast majority of cases (see Figure 1).
- Overall, the average self-assessed ratings for the three departments audited were assessed at a higher level of maturity, ranging mostly from upper-medium to high ratings. In contrast, the average audit ratings were significantly lower, ranging in the low end of the maturity spectrum (see Figure 1).
- For the departments audited, the variances observed between self-assessed and audit ratings were most significant in the CSE Top 10 security actions and incident management.

What was found for all areas assessed

Figure 1 depicts the average self-assessed ratings and average audit ratings in each of the areas assessed for all departments audited. It also includes the average self-assessed results of all participating departments. Maturity levels are defined in the Appendix B, Table B2. Through further analysis, the audit also noted the following:

- 27% of self-assessed ratings exceeded audit ratings by at least two maturity levels
- 37% of self-assessed ratings exceeded audit ratings by one full maturity level
- 35% of audit ratings were aligned with the self-assessed ratings

Figure 1: Small Departments (SDs) Self-Assessed Ratings versus Audit Ratings



Notes

a. It should be noted that results corresponding to question marks ("?") for maturity levels (considered a situational awareness issue) were counted as a zero in calculating maturity level averages for the purpose of this figure.

b. An overview of the areas covered by the self-assessment tool and the maturity levels can be found in Appendix B.

c. This line represents the average self-assessment ratings of the three departments audited.

d. This line represents the average OCG audit ratings of the three departments audited.

e. This line represents the average ratings of 35 small departments instead of all 36 small departments that completed the self-assessment. The results of one department were not reflected for security reasons.

▼ Figure 1 - Text version

Questions assessed in OCG Self-Assessment Tool [b]

Question [a]	Self-Assessment Ratings of 3 SDs [c]	OCG Audit Ratings [d]	Self-Assessment Ratings of 35 SDs [e]
1.1	2.3	1.3	2.1
1.2	2.3	2.0	2.1

Question [a]	Self-Assessment Ratings of 3 SDs [c]	OCG Audit Ratings [d]	Self-Assessment Ratings of 35 SDs [e]
1.3	2.3	1.7	2.1
1.4	1.7	1.3	1.7
1.5	2.0	0.7	1.4
1.6	1.3	0.7	1.7
1.7	2.7	0.7	2.2
1.8	2.3	0.3	1.8
2.1	2.0	1.0	1.9
2.2	2.3	1.0	2.1
2.3	2.7	2.0	2.2
2.4	2.0	2.0	1.6
2.5	1.7	0.7	1.4
3.1	2.0	1.3	1.9
3.2	2.0	1.3	2.0
3.3	1.7	1.3	1.5
3.4	1.7	0.7	1.7
3.5	2.0	1.3	1.6
3.6	2.3	0.3	1.5
3.7	2.0	0.3	1.1

Question [a]	Self-Assessment Ratings of 3 SDs [c]	OCG Audit Ratings [d]	Self-Assessment Ratings of 35 SDs [e]

Notes

[a] It should be noted that results corresponding to question marks (“?”) for maturity levels (considered a situational awareness issue) were counted as a zero in calculating maturity level averages for the purpose of this figure.

[b] An overview of the areas covered by the self-assessment tool and the maturity levels can be found in Appendix B.

[c] This line represents the average self-assessment ratings of the three departments audited.

[d] This line represents the average OCG audit ratings of the three departments audited.

[e] This line represents the average ratings of 35 small departments instead of all 36 small departments that completed the self-assessment. The results of one department were not reflected for security reasons.

Areas with the highest variance between the self-assessed and audited ratings

For the three departments audited, the top two areas with the highest variances between the small departments’ self-assessed ratings and the OCG’s audited ratings (see Figure 1) relate mainly to controls over the CSE

Top 10 security actions and incident management. Details of these areas are provided below.

CSE Top 10 security actions

The greatest variances observed in the areas assessed under the CSE Top 10 security actions [8] related to enforcing the management of the following:

- [Redacted] [9]
- [Redacted] [10]

Incident management

The greatest variances observed in this area were related to the following:

- **The processes for ensuring that lessons learned are documented and that the incident response plan is updated as needed (for example, following an incident):** Specifically, the variances observed were mainly due to unclear processes within two of the small departments [11] audited based on the supporting documentation provided and follow-up interviews conducted. As such, the OCG audit team assigned a low level of maturity to these controls, while two of the small departments audited self-assessed themselves at a high level of maturity, based on the assumption that these controls were covered under their agreement with third-party service providers. [12]
- [Redacted] [13]

Potential root causes

The following potential root causes were developed based on consultations with three additional small departments, [14] follow-up interviews, an examination of the supporting documentation provided by the departments audited, [15] and the OCG audit team's professional judgment. These potential root causes are not necessarily meant to be read as statements of fact but rather as potential factors that could help explain the variances observed.

Awareness of controls covered in agreements with third-party service providers

When departments assume that some IT security controls are covered by third-party service providers without verifying this assumption (with the agreements in place, for example), there is a risk that this assumption may lead to a false sense of security regarding these controls, which may, in reality, not be covered by anyone.

Lack of capacity and/or governance mechanisms

Small departments may not have timely access to IT security technical expertise needed and/or effective governance mechanisms to ensure that deputy heads are accurately briefed on the status of their organization's IT security controls in a manner that reflects the small department's unique IT security objectives and environment.

Low maturity for training and awareness

The low maturity observed in the training and awareness area (as depicted in Figure 1) indicates a lack of formalized IT security training that may lead to a misinterpretation of lead security agencies' guidance and create a situational awareness gap, which in turn could explain the variances observed.

Conclusion

Overall, the audit noted that all three of the small departments audited overestimated, to varying degrees, the maturity of their IT security controls. The areas with the most significant variances between the self-assessment ratings and the audit ratings were the following:

- **CSE Top 10 security actions**, [Redacted]
- **incident management**, including documentation of lessons learned and incident response plans being updated as needed or following an incident

There is a risk that other small departments that have also completed the same self-assessment but were not included in this audit could observe similar overestimation trends within their own department. The reason for these overestimations could be explained by a multitude of factors, including but not limited to the following:

- relying on unverified assumptions about the extent of controls covered by third-party providers (leading to a situational awareness gap)
- lack of training
- not having timely access to IT security technical expertise to accurately assess the state of technical controls in place
- lack of effective governance mechanisms to ensure that deputy heads are accurately briefed on the status of their organization’s IT security controls

Recommendations

1. [Redacted] should ensure that they have a documented process in place to regularly review and update (where appropriate and to the extent feasible) their service agreement(s) with third-party IT service providers. During these regular reviews and updates, consideration

should be given to ensuring the following, where appropriate and to the extent feasible:

i. IT security services and controls covered (including those excluded) by third-party providers are identified and described in the agreement(s)
ii. roles and responsibilities are identified and described in the agreement(s)
iii. service standards and reporting requirements expected of third-party service providers are identified and described in the agreement(s)
iv. departmental security risks and control profiles are reassessed, with any relevant updates reflected in the agreements
v. the latest version(s) of agreement(s) in place with third-party IT service providers are communicated to all relevant departmental stakeholders that have IT security responsibilities

2. To help further facilitate a consistent and accurate assessment of IT security maturity, all departments included in this audit should ensure that formal standardized monitoring and reporting frameworks are in place and that senior designated departmental executives (including deputy heads) are regularly briefed on the results of these monitoring activities, as well as on the status of any remedial actions deemed appropriate according to the department’s risk tolerance. At a minimum, such briefings should cover the implementation of the CSE Top 10 security actions [16] to the extent deemed appropriate based on the department’s risk tolerance and available resources.

   Responsibilities for performing monitoring and reporting activities should also be segregated, to the extent possible, from the individuals responsible for implementing the IT security controls assessed.

General advice for all small departments

This section provides general advice for all small departments based on the analysis of self-assessment results received (from 36 small departments) and the subsequent follow-up audit work completed by the OCG in a targeted sample of these departments.

1. When relying on self-assessments, consider the risk of overestimation in maturity levels:
    - consider that based on the targeted follow-up audit work performed by the OCG:
        - the majority of the departments audited overestimated their self-assessment results by at least one maturity level
        - results were significantly overstated in the areas of the CSE Top 10 security actions and incident management
    - ensure that available training from lead security agencies is leveraged to help mitigate the risk of overestimation; examples include the Canadian Centre for Cyber Security’s Learning Hub and the Canada School of Public Service (see Appendix F for additional resources)
2. Assess the applicability of the audit recommendations:
    - all small departments that were not scoped into this targeted audit are strongly encouraged to assess the applicability of the recommendations provided in this report within their respective context and to develop, as well as follow up internally on, management action plans where appropriate
3. Leverage pre-established tools to further facilitate a regular and structured monitoring of IT security controls:
    - all departments should consider regularly leveraging existing tools for this purpose; examples of relevant existing tools would include but not be limited to the following:

        - OCG self-assessment tool
        - CSE standard security control profiles or other tools issued by lead security agencies (Treasury Board of Canada Secretariat, CSE, Shared Services Canada)

      Further examples are provided in Appendix G.
    - Where applicable and to the extent feasible, departments should develop and/or use customized tools adapted specifically to their risk environment in order to consistently assess the state of IT security controls in areas deemed key and in alignment with policy requirements

Management response

The findings and recommendations of this audit were presented to the three audited small departments and the three consulted small departments that participated in this audit.

Management has agreed with the findings set out in this report and will take action to address all applicable recommendations.

Conformity statement

This internal audit was conducted in conformance with the International Standards for the Professional Practice of Internal Auditing.

Mike Milito, MBA, CIA, CRMA
Assistant Comptroller General and Chief Audit Executive
Internal Audit Sector, Office of the Comptroller General

Appendix A: list of departments scoped into the mandatory OCG self-assessment

Table A1: Abbreviations and names of small departments scoped into the mandatory OCG self-assessment

Abbreviation	Name of small department [*]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]

[*] The OCG identified 47 small departments. However, 11 small departments were excluded from the self-assessment because they had their own audit function, were inactive or no longer exist.

Abbreviation	Name of small department [*]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]

[*] The OCG identified 47 small departments. However, 11 small departments were excluded from the self-assessment because they had their own audit function, were inactive or no longer exist.

Abbreviation	Name of small department [*]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]

[*] The OCG identified 47 small departments. However, 11 small departments were excluded from the self-assessment because they had their own audit function, were inactive or no longer exist.

Appendix B: overview of areas covered by the self-assessment tool

▼ In this section

Table B1: Areas covered by the self-assessment tool and question descriptions

Area	No.	Question description

Area	No.	Question description
1a. Governance	1.1	Departmental oversight bodies for the management of IT security have been established and are operating as intended.
	1.2	An approved departmental plan that covers IT security is in place. The plan aligns with government-wide policies and departmental priorities, and is communicated to all stakeholders.
	1.3	Departments should ensure that accountabilities, roles and responsibilities related to IT security have been formally established and communicated.
	1.4	A human resources (HR) plan that includes consideration of IT security professionals has been established.

Area	No.	Question description
1b. CSE Top 10 security actions	1.5	The department’s approach to managing IT security risks includes the following key elements, based on the approach recommended by the Communications Security Establishment’s (CSE’s) ITSG-33 Annex 1: a. evidence of a departmental IT security threat risk assessment that has been reviewed in the past year b. development of a departmental security control profile c. monitoring and assessment of the performance of security controls, continuous assessment activities (such as vulnerability assessment) d. the ability to report on the status of security assessment and authorization across their applications, whether critical or not
	1.6	The department regularly monitors the extent to which it has implemented all of the CSE Top 10 IT security actions and adopts corrective measures to address any gaps identified in consideration of the relevant risks.
	1.7	[Redacted]
	1.8	[Redacted]

Area	No.	Question description
2. IT security training and awareness	2.1	A departmental IT security awareness and training program that is role-based in nature is in place and meets the needs of the department. Examples of roles include general user, IT security specialist and developer.
	2.2	The departmental IT security awareness and training program covers the following key areas: a. safe web browsing b. social engineering c. phishing d. password selection and protection
	2.3	The department has a process in place to regularly remind employees of their IT security responsibilities.
	2.4	The department has a process in place to regularly monitor and track the level of completion of the IT security awareness and training program and ensure the training has been completed.
	2.5	The department measures the effectiveness of its IT security awareness and training program and has a remediation process to support continual improvement.

Area	No.	Question description
3. Incident management	3.1	The department has documented accountabilities, roles and responsibilities for the detection of IT security incidents (“who” detects “what”).
	3.2	The department has established a process to identify and assess IT security incidents in a timely manner.
	3.3	The department has established an incident response plan that is executed when an IT security incident occurs.
	3.4	The department has established an incident response process to ensure that IT security incidents are reported to the appropriate stakeholders.
	3.5	The department has a plan to ensure that it can recover from IT security incidents in a timely manner.
	3.6	The department has established a process to ensure that after an IT security incident occurs, lessons learned are documented (post-event activity) and the incident response plan is updated as needed.
	3.7	[Redacted]

Description of IT security maturity levels

The maturity level specifies the path that a process follows in moving from an early-stage and ad hoc process to a highly mature process. Each level of maturity provides a set of goals that, when met, places an organization at the next level of maturity. It also establishes certain characteristics for processes, procedures or activities that are required for each maturity level. As such, higher maturity levels will present more advanced characteristics and can be seen as a step toward achieving a mature process.

Table B2 presents examples of what each level of maturity entails.

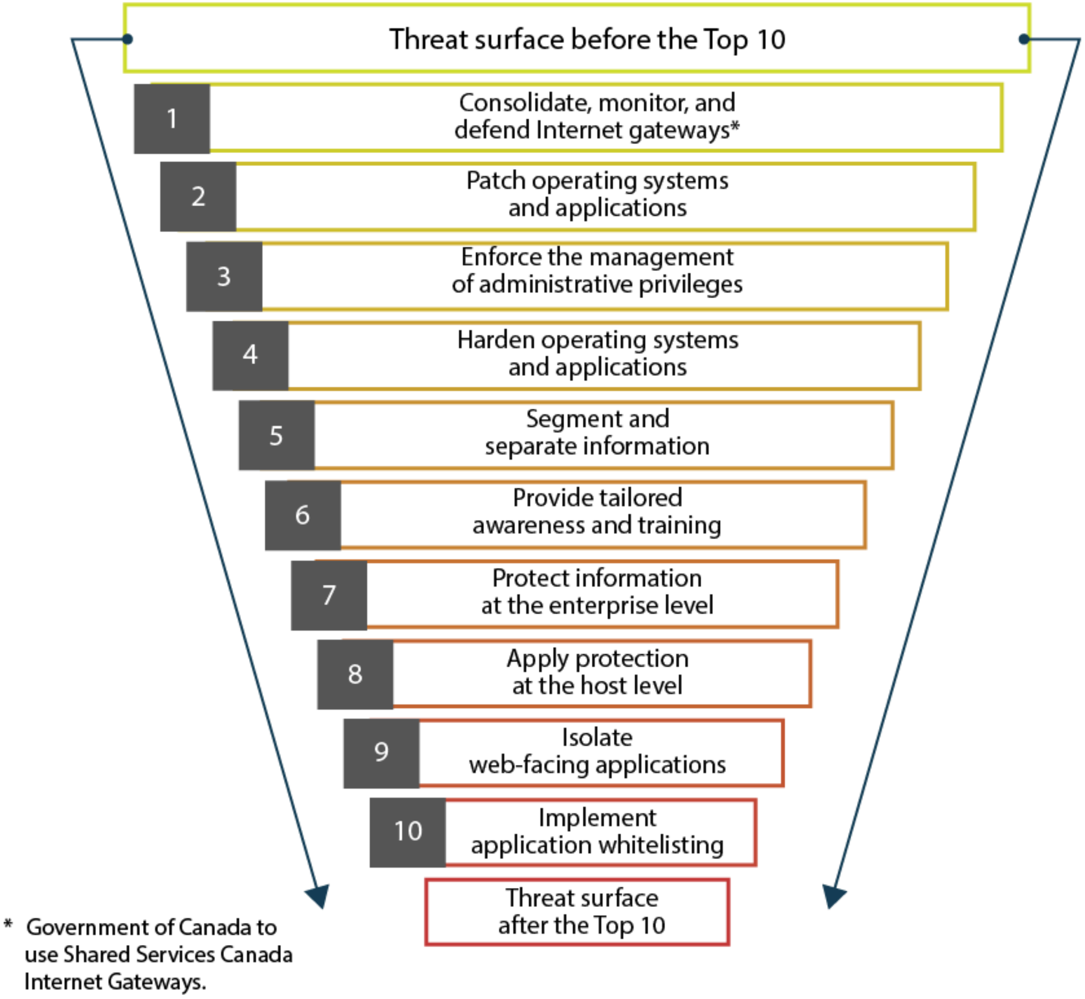
Table B2: examples of what maturity levels entail

Level 3: High	• Formal, documented and approved IT security-related process(es), program(s) or plan(s) are in place that are monitored, tested, updated, reported on and overseen by governance bodies. • All IT security roles and responsibilities are formally defined, documented, approved and communicated. • Formal and established governance bodies exist, and IT security-related issues are discussed regularly.
Level 2: Medium	• There are some formal and approved IT security process(es), program(s) or plan(s), but they are reported, monitored and updated only on an ad hoc basis. • Some roles and responsibilities are formally defined, documented, approved and communicated. • Formal and established governance bodies discuss IT security-related issues on an ad hoc basis.
Level 1: Low	• Documented procedures, process(es) or formal and approved plan(s) do not exist. • There are no defined IT security roles and responsibilities. • Monitoring or reporting of specific IT security-related process or activity does not exist.

Unknown: ?	A question mark (“?”) was selected if the small department was unsure of its level of maturity (there was a situational awareness gap).

Appendix C: Communications Security Establishment Top 10 security actions

Figure C1: Communications Security Establishment Top 10 security actions


Threat surface before the Top 10
1
Consolidate, monitor, and defend Internet gateways*
2
Patch operating systems and applications
3
Enforce the management of administrative privileges
4
Harden operating systems and applications
5
Segment and separate information
6
Provide tailored awareness and training
7
Protect information at the enterprise level
8
Apply protection at the host level
9
Isolate web-facing applications
10
Implement application whitelisting
Threat surface after the Top 10
* Government of Canada to use Shared Services Canada Internet Gateways.

▼ Figure C1 - Text version

This image demonstrates the Top 10 security actions from Communications Security Establishment to reduce the threat surface in GC networks.

Threat surface before the Top 10

1. Consolidate, monitor, and defend Internet gateways (Note: Government of Canada to use Shared Services Canada Internet Gateways)
2. Patch operating systems and applications
3. Enforce the management of administrative privileges
4. Harden operating systems and applications
5. Segment and separate information
6. Provide tailored awareness and training
7. Protect information at the enterprise level
8. Apply protection at the host level
9. Isolate web-facing applications
10. Implement application whitelisting

Threat surface after the Top 10

As identified in ITSB-89 V3, *Top 10 IT Security Actions to Protect GC Internet-Connected Networks and Information*, implementation of the CSE Top 10 security actions will eliminate the vast majority of cyber threats currently seen as active in GC networks.

Appendix D: Summary of small departments' self-assessment results

▼ In this section

A summary of small departments' self-assessment results is as follows:

- Overall, each self-assessed criterion averaged close to a medium level of maturity, with an overall 49% of respondents indicating a Level 2 for most questions.
- There is a global situational awareness gap average of 7%, which is considered high. This gap is due to the fact that some departments were not able to provide answers to certain self-assessment questions and can be an indication of limited control or knowledge of their departmental IT security status.
- Small departments have rated themselves lower in the most technical areas of the self-assessment, such as the CSE Top 10 security actions and incident management. Consequently, these areas also have the largest situational awareness gap at 10% each; therefore, both are 3% above the average.

7% of questions were assessed as "? – Unknown" by the departments.

IT security governance

- A large majority of small departments indicated having the following:
  - departmental oversight bodies
  - a plan that covers IT security
  - formally defined and understood IT security accountabilities

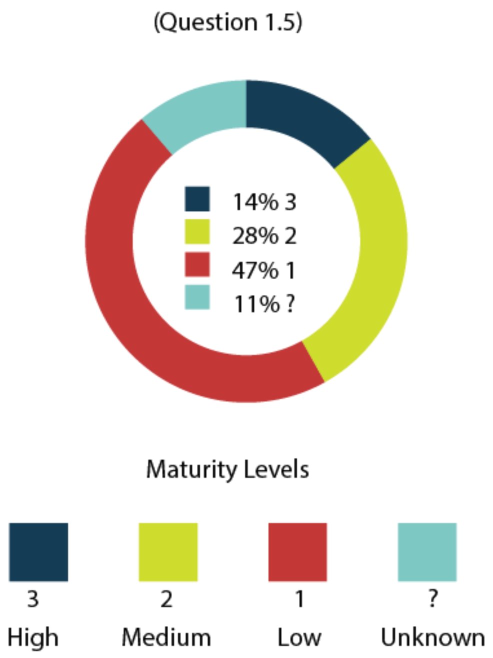
  - clear roles and responsibilities

78% of departments indicated a medium to high level of maturity for all four sub-criteria covered by governance (1.1–1.4).

CSE Top 10 security actions

- Only 14% have indicated a high level of maturity for having implemented key elements recommended by CSE ITSG-33 Annex 1, while 11% are unaware of what has been implemented in their organization.
- 75% of small departments mentioned that they monitor some or all CSE Top 10 security actions and report any gaps to senior management.
- 53% of small departments have indicated having a high level of maturity for managing [Redacted].
- For the [Redacted], 81% of small departments have indicated a medium to high level of maturity. However, only 12% mentioned using [Redacted].

Figure D1: Implementation of CSE Top 10 security actions by small departments and maturity level



▼ Figure D1 - Text version

Implementation of CSE Top 10 security actions by small departments and maturity level

14% indicated a high level of maturity

28% indicated a medium level of maturity

47% indicated a low level of maturity

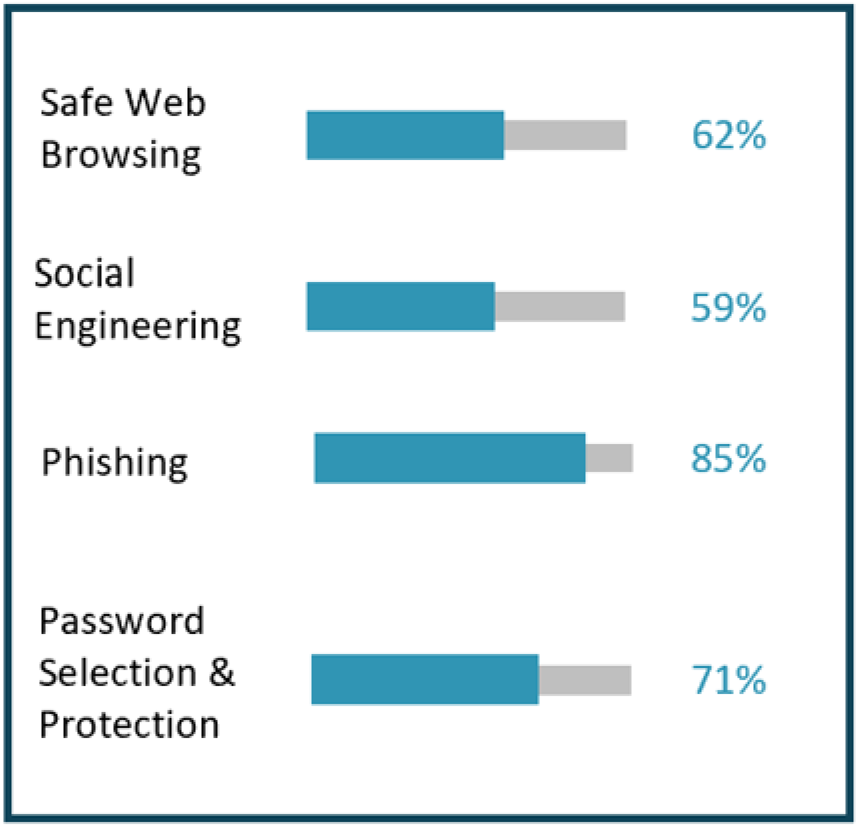
11% indicated an unknown level of maturity

IT security training and awareness program

- The majority of small departments indicated having a departmental security and awareness training program, including 85% of small departments addressing phishing within their program. However, only 42% mentioned implementing a program that covers all four key security and awareness training areas. Only 14% of the departments mentioned having a regularly reviewed and updated role-based training and awareness program.

- Nearly all small departments stated that they remind their employees of their IT security responsibilities, with about one third having a formally approved and documented process.
- None of the respondents indicated the presence of an approved and documented process to measure the effectiveness of the program. This question yielded the lowest self-assessed overall maturity of all questions in this area and was consistent across departments.
- Only 56% of small departments indicated having a medium or high level of maturity for monitoring employee participation in and completion of IT security training.

Figure D2: Percentage of small departments that have an IT security and awareness program that covers four areas



▼ Figure D2 - Text version

Percentage of Small Departments with an IT Security Training and Awareness Program that covers the following Key Areas:

Safe Web Browsing	62%
Social Engineering	59%
Phishing	85%
Password Selection & Protection	71%

Incident management

- A large majority of small departments indicated that they have defined and communicated their roles and responsibilities for incident detection and have a process to identify and assess IT security incidents.
- Only 13% of responses indicated a high level of maturity for incident management (lowest among all four areas covered by the self-assessment).
- 56% of small departments indicated having an incident response plan, but only a [Redacted]. Only two small departments reported having a mature plan that is regularly reviewed and updated.
- Only 6% of small departments indicated that they have a plan to recover from IT security incidents in a timely manner.
- 61% of small departments indicated documenting lessons learned.

13% of incident management criteria responses were self-assessed at a high maturity level (3).

Appendix E: Sampling approach

▼ In this section

Departments selected for validation

Based on the analysis of the completed self-assessments, the OCG identified small departments that indicated the highest relative level of maturity in response to the 20 questions in the self-assessment as follows:

- overall maturity (high in terms of the highest average maturity across all 20 questions)
- questions that consistently received lower scores across almost all small departments (four or fewer small departments rated their department as having a maturity level of 3 on that particular question)

From this subset of departments, the OCG's selection was prioritized based on risk, verifiability, value-added and representation. Factors in determining prioritization were as follows:

- representation across the peer groups (small, medium, large or Regional Development Agency)
- representation of service delivery model (in-house, Shared Services Canada, third party or a combination)
- sensitivity of information handled and public-facing nature of departmental applications
- verifiability in terms of the availability of documentation provided in support of the completed self-assessments

- existence of potential best practices
- whether the small department was scoped into the previous IT security audit (departments previously scoped into that audit were not prioritized)

Two small departments were selected based on the priorities described above, and an additional small department from the group of small departments that self-assessed at greater than 1.5 in terms of average maturity (medium level maturity) was added. The three departments scoped for validation of the self-assessment results were:

- [Redacted]
- [Redacted]
- [Redacted]

Departments selected for consultation

The consultation sample was selected from the small departments that self-assessed at a low level of maturity in one or more areas or were “outliers” in terms of their responses to questions in specific areas. The three small departments chosen for consultation were selected after analysis of the completed self-assessments, and each of the chosen departments should satisfy one of the following criteria:

- department with an overall low level of maturity across all four areas
- department with a low level of maturity in one area while all other areas are at a medium to high level of maturity
- department with “?” responses for all questions in one or two areas

The three small departments scoped into consultations were as follows:

- [Redacted]
- [Redacted]
- [Redacted]

The consultations took the form of structured interviews that explored root causes and other challenges experienced by those departments that reported very low levels of maturity for specific or all areas of the self-assessment, depending on which selection criteria, specified above, they qualified for. The key factor in selecting these departments for consultation was value added.

Appendix F: IT security training and awareness resources

The links in Table F1 are provided for information purposes only. Information available through these links could be leveraged by departments to help enhance their IT security training and awareness programs.

Table F1: IT security training and awareness resources

Type of resources	Source	Link
Videos, courses and seminars for GC employees at no cost to learners (“Security Awareness” (A230) is a popular course)	Canada School of Public Service, Government of Canada	Canada School of Public Service
Learning Hub, Get Cyber Safe website, Cyber Security Awareness Month, Introduction to the Cyber Threat Environment	Canadian Centre for Cyber Security, Government of Canada	Learning Hub Get Cyber Safe Cyber Security Awareness Month An introduction to the cyber threat environment

Type of resources	Source	Link
Information on recent scams and frauds	Canadian Anti-Fraud Centre, Government of Canada	Canadian Anti-Fraud Centre
Information on threats to national security	Royal Canadian Mounted Police, Government of Canada	National Security Awareness
Information sheets on various topics related to IT, training resources, events, opportunities and more	Information Systems Audit and Control Association (ISACA) website	Information Systems Audit and Control Association (ISACA)
Videos and consumer alerts	Federal Trade Commission, United States Government	Federal Trade Commission Consumer Advice
Tip sheets, posters and videos on online security	Stop Think Connect, United States	Stop Think Connect
Tips on creating strong passwords	Educause Review	8 Do’s and Don’ts of Good Passwords
Microsoft email security	Microsoft	Top 6 email security best practices to protect against phishing attacks and business email compromise

Type of resources	Source	Link
Various resources on cybersecurity	Educause	Cybersecurity Awareness Resource Library
Information on IT, training resources, events, opportunities and more	National Institute of Standards and Technology (NIST), United States	National Initiative for Cybersecurity Education (NICE)
Infographics, templates, toolkit and videos	National Cyber Security Centre, United Kingdom	National Cyber Security Centre

Appendix G: IT security tools available from lead security agencies

Table G1: IT security tools available from lead security agencies

Type of tool	Source	Link
Cyber Security Applications Portal (Beta) **Provides federal departments access to an integrated set of digital cyber security tools**	Treasury Board of Canada Secretariat: Application Portal Home	TBS Applications Portal (TAP)

Type of tool	Source	Link
Enterprise Security Architecture (ESA) tools and templates	Treasury Board of Canada Secretariat, Government of Canada	ESA Tools and Templates (accessible only on the Government of Canada network)
CSE security profiles	Canadian Centre for Cyber Security, Government of Canada	Suggested organizational security control profile for departments and agencies that require protection of business activities of security category Protected B, medium integrity and medium availability: Annex 4A - Profile 1 - (PROTECTED B / Medium integrity / Medium availability) (ITSG-33) Excel spreadsheet working document: Suggested security controls and control enhancements (ITSG-33) Security profile for guidance on the security categorization of cloud-based services: *Guidance on the security categorization of cloud-based services (ITSP.50.103)* Baseline cyber security controls for small and medium organizations

Type of tool	Source	Link
Government of Canada (GC) Cloud Brokering Services Resource for GC departments and agencies to obtain trusted public cloud services for classified and secure data	Shared Services Canada, Government of Canada	Government of Canada (GC) Cloud Brokering Services

Footnotes

[1] Assurance activities involve the internal auditor's objective assessment of evidence to provide opinions or conclusions regarding an entity, operation, function, process, system or other subject matters. Consulting activities are conducted to provide timely insight to inform management's decision; oversight and foresight are advisory in nature and negotiated with the engagement client.

[2] The review focused on the following: *Digital Operations Strategic Plan: 2018-2022* and *Policy on Service and Digital*.

[3] Appendix A provides a list of these 36 participating small departments and a rationale for the exclusion of 11 small departments from the self-assessment exercise.

4 Appendix B lists the areas covered by the self-assessment tool and the maturity levels.

5 Appendix C describes the CSE Top 10 IT security actions.

6 Appendix A provides a list of these 36 participating small departments and a rationale for the exclusion of 11 small departments from the self-assessment exercise.

7 The OCG placed each department in a peer group in order to better illustrate where they stand in relation to other departments that are the most similar to them. This was done by using each department's Actual Spending and Actual Full Time Equivalents (FTE) data from their 2017-18 Departmental Results Report in order to form groupings. Based on this information, the OCG established four peer groups for small departments: small, medium, large, and regional development agency.

8 It should be noted that the OCG self-assessment tool did not assess all 10 areas within the CSE Top 10 security actions presented in Appendix C. It focused on the following four areas: *IT Security Risk Management: A Lifecycle Approach (ITSG-33)*, monitoring of the CSE Top 10 security actions implementation, [Redacted].

9 [Redacted]

10 [Redacted]

11 [Redacted]

[12] For the purpose of this audit, the term “third-party service provider” is used broadly in reference to other department(s) with responsibilities (where applicable) for delivering IT services to the small departments audited (for example, Shared Services Canada or a parent or portfolio department).

[13] [Redacted]

[14] The additional small departments included in the consultation on potential root causes were [Redacted]. Refer to Appendix A for details.

[15] The small departments included in the audit were [Redacted]. Refer to Appendix A for details.

[16] Refer to Appendix C for details.

Date modified:
2022-10-04