SCoE Security Centre of Excellence

Security Centre of Excellence SCoE·CEeS Centre d'excellence en sécurité

A look at the role of the SCoE

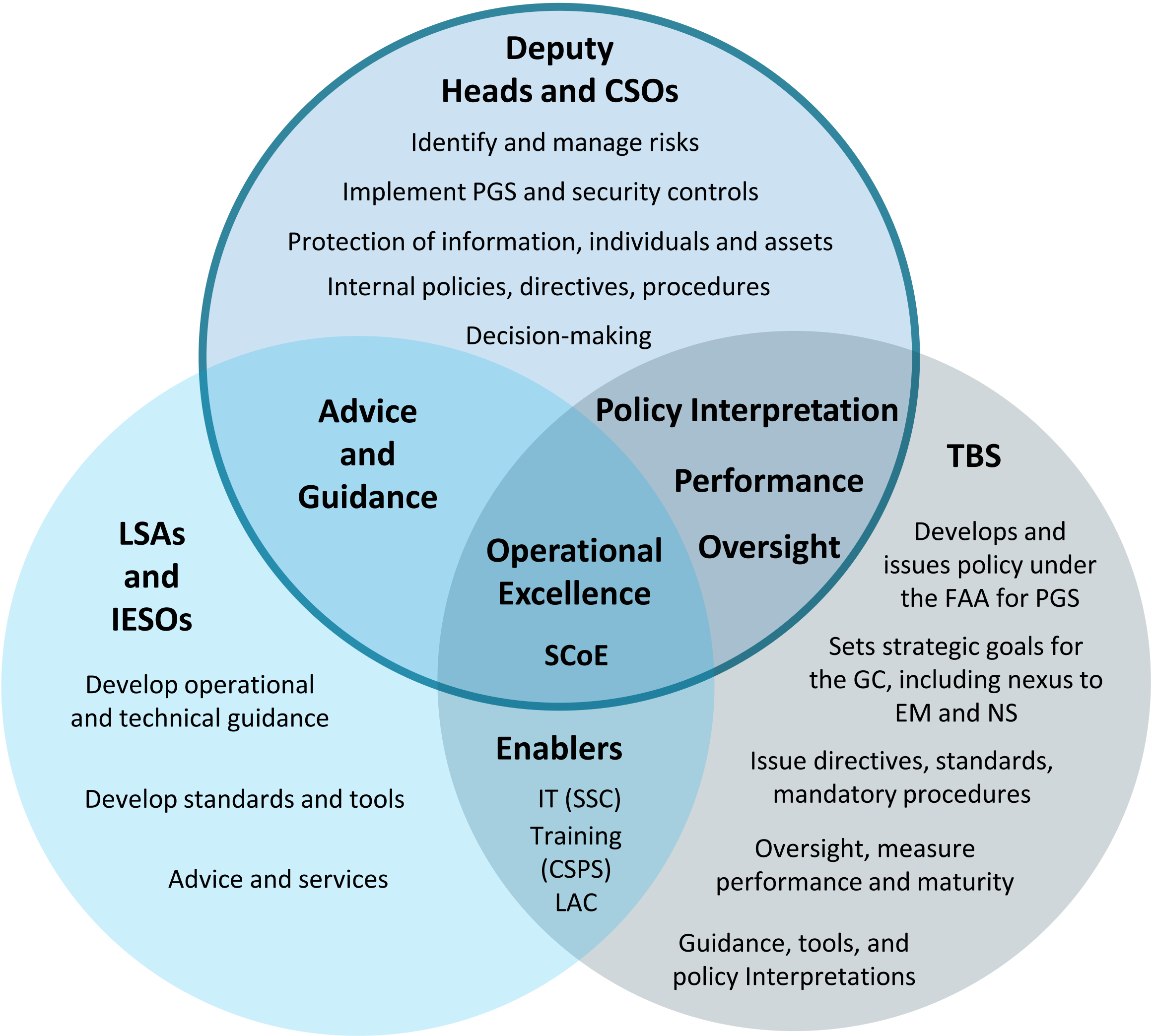
Canada

Background and context

- The SCoE, formerly known as the DSO Centre for Development (CfD), has been in operation since 2012
- Its mandate was renewed in 2022 by the National Security and Intelligence Advisor (NSIA) to the Prime Minister for 5 additional years
- Mission: To lead the development of a knowledgeable, resilient and integrated security community across the Government of Canada (GC)
- Housed in PCO, the SCoE supports:
  - GC Chief Security Officers (CSO) and a community comprised of approximately 3500 security officials
  - NSIA's role as the Champion of Government Security
  - LSAs mandate in the provision of agile operational guidance and the delivery of learning/networking events, including PCO's LSA role for Readiness through the design and facilitation of various exercises
  - Broader Security and Intelligence information sharing and GC response objectives

SCoE Security Centre of Excellence

Strength of the SCoE


Deputy Heads and CSOs
Identify and manage risks
Implement PGS and security controls
Protection of information, individuals and assets
Internal policies, directives, procedures
Decision-making
Advice and Guidance
Policy Interpretation
Performance
Oversight
TBS
Develops and issues policy under the FAA for PGS
Sets strategic goals for the GC, including nexus to EM and NS
Issue directives, standards, mandatory procedures
Oversight, measure performance and maturity
Guidance, tools, and policy Interpretations
LSAs and IESOs
Develop operational and technical guidance
Develop standards and tools
Advice and services
Operational Excellence
SCoE
Enablers
IT (SSC)
Training (CSPS)
LAC

- At the heart of community, the SCoE acts on behalf of departments as a catalyst and surge capacity to tackle their operational needs
- As functional lead, it draws from all the resources available to develop tools and innovative solutions that have been vetted by LSAs and TBS
- Being housed at PCO, the SCoE offers a unique perspective on security challenges
- It has a strong governance in place that enables it to achieve results and add value
- It is forward-thinking, going beyond existing policies
- It is agile and has demonstrated capacity to deliver meaningful work in short periods of time

Excellence in Security: #Ready and Prepared

Strategic Objectives

Community

Establish a centralized « Community Centre » where security practitioners can build or enhance their networks through information sharing and collaboration to support government-wide security readiness;

People

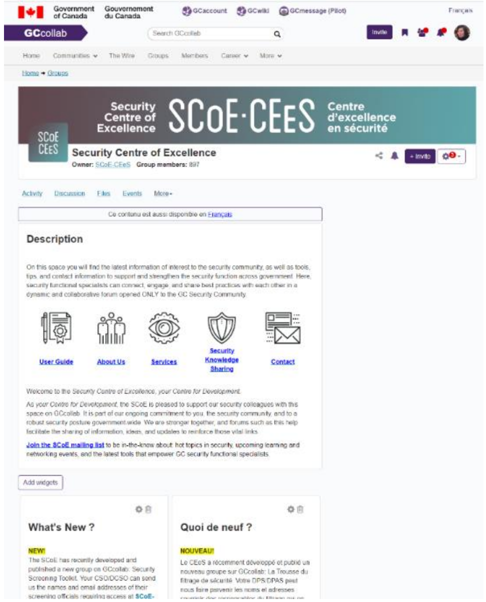
Strengthen human capital through education, exercise, training and mentoring, and sustain a capable and learning security workforce, able to mitigate known and emerging risks

Knowledge

Leverage collective understanding of Canada's security landscape to support and improve government-wide resilience.

SCoE Security Centre of Excellence

Stronger together
Connecting the community



Security Centre of Excellence

Owner: SCoE-CEeS Group members: 897

Ce contenu est aussi disponible en Français

Description

On this space you will find the latest information of interest to the security community, as well as tools, tips, and contact information to support and strengthen the security function across government. Here, security functional specialists can connect, engage, and share best practices with each other in a dynamic and collaborative forum opened ONLY to the GC Security Community.

User Guide | About Us | Services | Security Knowledge Sharing | Contact

Welcome to the *Security Centre of Excellence, your Centre for Development.*

As *your Centre for Development*, the SCoE is pleased to support our security colleagues with this space on GCcollab. It is part of our ongoing commitment to you, the security community, and to a robust security posture government-wide. We are stronger together, and forums such as this help facilitate the sharing of information, ideas, and updates to reinforce those vital links.

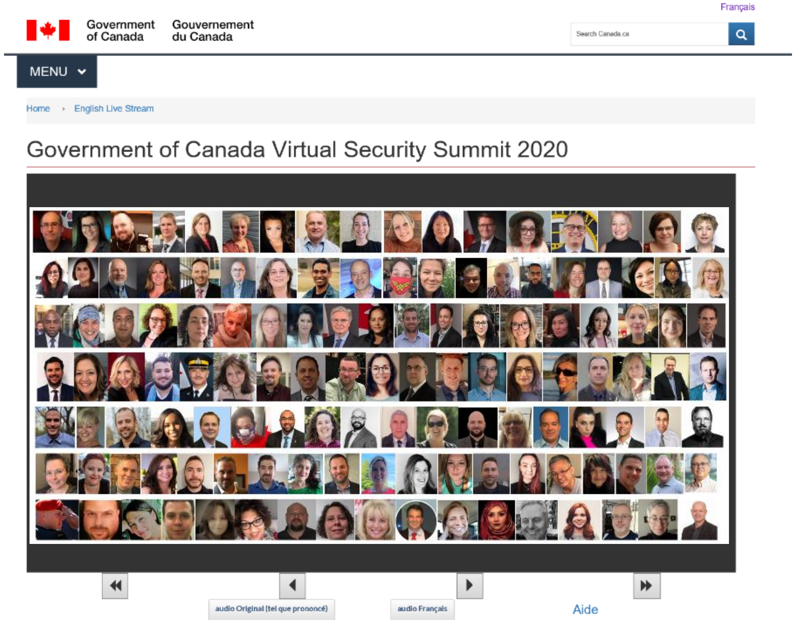
Join the SCoE mailing list to be in-the-know about: hot topics in security, upcoming learning and networking events, and the latest tools that empower GC security functional specialists.

What's New ?

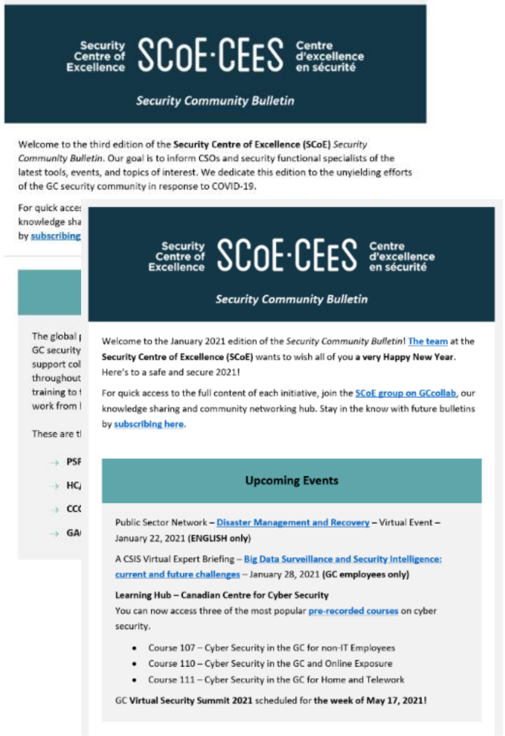
NEW!
The SCoE has recently developed and published a new group on GCcollab: Security Screening Toolkit. Your CSO/DCSO can send us the names and email addresses of their screening officials requiring access at SCoE-

Quoi de neuf ?

NOUVEAU!
Le CEeS a récemment développé et publié un nouveau groupe sur GCcollab: La Trousse du filtrage de sécurité. Votre DPS/DPAS peut nous faire parvenir les noms et adresses


Français
Government of Canada Gouvernement du Canada
Search Canada.ca
MENU
Home › English Live Stream
audio Original (tel que prononcé)
audio Français
Aide

Government of Canada Virtual Security Summit 2020


Security Centre of Excellence SCoE·CEES Centre d'excellence en sécurité

Security Community Bulletin

Welcome to the third edition of the **Security Centre of Excellence (SCoE)** *Security Community Bulletin*. Our goal is to inform CSOs and security functional specialists of the latest tools, events, and topics of interest. We dedicate this edition to the unyielding efforts of the GC security community in response to COVID-19.

Security Community Bulletin

Welcome to the January 2021 edition of the *Security Community Bulletin*! The team at the **Security Centre of Excellence (SCoE)** wants to wish all of you **a very Happy New Year**. Here's to a safe and secure 2021!

For quick access to the full content of each initiative, join the SCoE group on GCcollab, our knowledge sharing and community networking hub. Stay in the know with future bulletins by **subscribing here**.

Upcoming Events

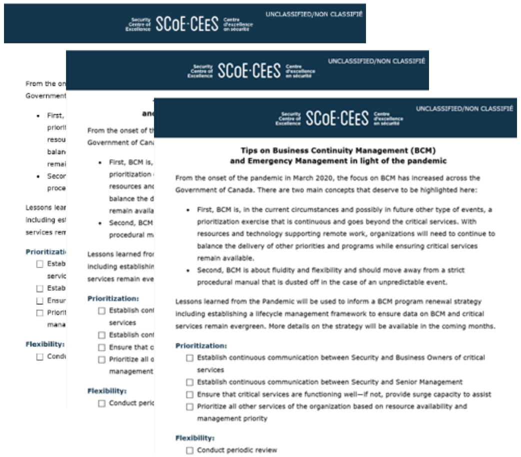
Public Sector Network – Disaster Management and Recovery – Virtual Event – January 22, 2021 (**ENGLISH only**)

A CSIS Virtual Expert Briefing – Big Data Surveillance and Security Intelligence: current and future challenges – January 28, 2021 (**GC employees only**)

Learning Hub – Canadian Centre for Cyber Security
You can now access three of the most popular pre-recorded courses on cyber security.

- Course 107 – Cyber Security in the GC for non-IT Employees
- Course 110 – Cyber Security in the GC and Online Exposure
- Course 111 – Cyber Security in the GC for Home and Telework

GC **Virtual Security Summit 2021** scheduled for **the week of May 17, 2021!**


Security Centre of Excellence SCoE·CEES Centre d'excellence en sécurité
UNCLASSIFIED/NON CLASSIFIÉ

Tips on Business Continuity Management (BCM) and Emergency Management in light of the pandemic

From the onset of the pandemic in March 2020, the focus on BCM has increased across the Government of Canada. There are two main concepts that deserve to be highlighted here:

- First, BCM is, in the current circumstances and possibly in future other type of events, a prioritization exercise that is continuous and goes beyond the critical services. With resources and technology supporting remote work, organizations will need to continue to balance the delivery of other priorities and programs while ensuring critical services remain available.
- Second, BCM is about fluidity and flexibility and should move away from a strict procedural manual that is dusted off in the case of an unpredictable event.

Lessons learned from the Pandemic will be used to inform a BCM program renewal strategy including establishing a lifecycle management framework to ensure data on BCM and critical services remain evergreen. More details on the strategy will be available in the coming months.

Prioritization:
- ☐ Establish continuous communication between Security and Business Owners of critical services
- ☐ Establish continuous communication between Security and Senior Management
- ☐ Ensure that critical services are functioning well—if not, provide surge capacity to assist
- ☐ Prioritize all other services of the organization based on resource availability and management priority

Flexibility:
- ☐ Conduct periodic review

Canada

Operational Excellence

PCO is responsible for the oversight of the SCoE **administrative activities & expenditures**

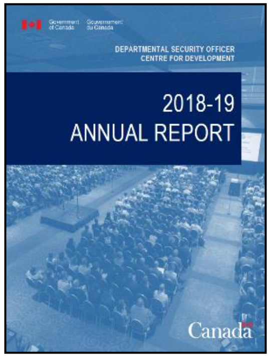
Governance via a Board of Management comprised of 6 CSO's representative approving priorities, work plans and annual reports, and a Board of Directors comprised of 4 LSA representatives who provide strategic direction

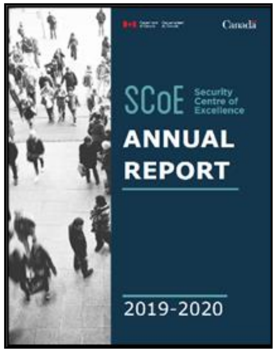
Budget of approximately 1,5M$/FY via 92 MoUs

- 30K for large organizations (over 5,000 employees)
- 20K for medium organizations (1,000 to 5,000 employees)
- 10K for small organizations (100 to 1,000 employees)
- 5K for micro organizations (less than 100 employees)

Results-based organization where performance is measured regularly and targets set. The community is very satisfied with the services, the value for money and return on investment. They has been significant growth in all services

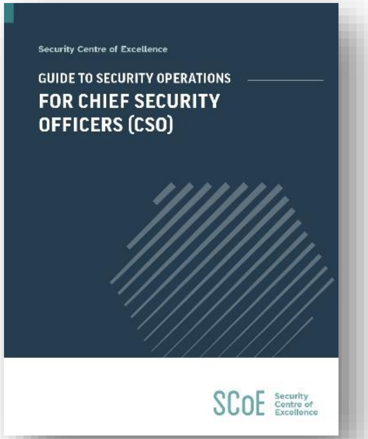
Operate with a mixed **human resources management strategy** (indeterminate, secondment and term employees) to ensure that the organization remains relatively small and adapts to changes to security priorities, while staying within the level of funding provided by the community


Government of Canada Gouvernement du Canada
DEPARTMENTAL SECURITY OFFICER
CENTRE FOR DEVELOPMENT
2018-19
ANNUAL REPORT
Canada



SCoE Security Centre of Excellence
2021-22
ANNUAL REPORT
Government of Canada Gouvernement du Canada
Canada

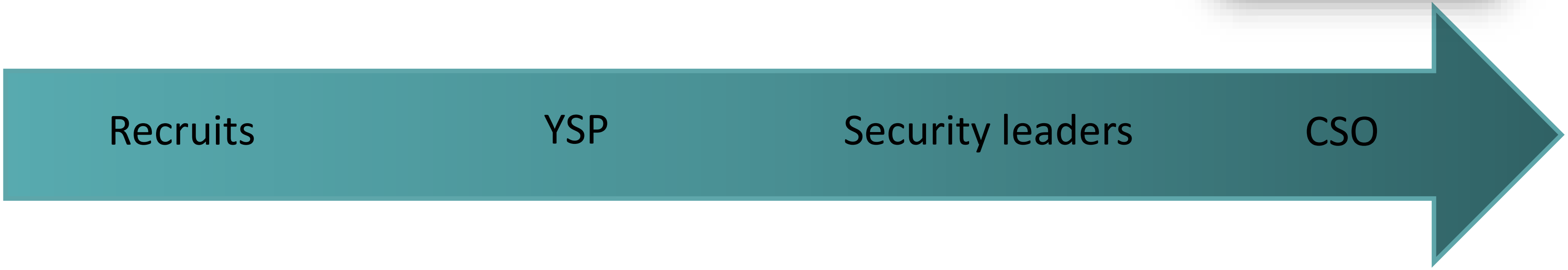
For the whole community



Security Centre of Excellence

GUIDE TO SECURITY OPERATIONS
FOR CHIEF SECURITY
OFFICERS (CSO)

SCoE Security Centre of Excellence



Recruits

- Reviewing curriculum
- Cooperating with PSC
- Creating meeting ground (speed networking, career fair, etc.)

YSP

- Networking
- Learning activities
- Showcasing their work

Security leaders

- Continuous learning
- Providing tools
- Offering guidance

CSO

- Orientation session
- CSO Guide to Security Operation
- Offering advice

SCoE Security Centre of Excellence

Supporting operations with advice and guidance

Equipping community with knowledge

REQUEST PROCESS

Requests are submitted to the Centre

- **Requests are received** via various sources:
  - Emails
  - Phone calls
  - In person meetings (Outreach, Events, etc.)
- **Requests are logged** into a tracker with metadata:
  - Name of requester
  - Name of organization
  - Date received
  - Summary of request
  - Relevant security control or other
  - Name of SCoE responder
  - Follow up required Y/N

VALIDATION PROCESS

Requests are validated to ensure the scope and nature is well understood

- **Requesters are contacted** to validate their needs and expectations
- **Scope and nature criteria** assist the Research & Analysis Process:
  - Organization sizes
  - Organization business lines
  - Timelines and priorities
  - National VS organizational components
  - Nature (sharing existing material VS development of new material)
- **Requests outside of SCoE mandate** are relayed to the appropriate authority (CLEL, LSA, etc…)
- **Agreement on the way forward** with the requester (if needed)

RESEARCH & ANALYSIS PROCESS

Research and analysis is conducted to gather and share relevant and up-to-date information

- **Research is initiated internally** using various sources:
  - SCoE tracker
  - SCoE shared drives
  - PCO InfoXpress, GCdocs, InfoNet
  - PCO library
  - GC tools (GCconnex, GCcollab, GCpedia, GCintranet…)
- **Research is initiated externally** using various sources:
  - Open sources
  - Shared GC ressources
  - Other non-GC sites/collections (Conference Board of Canada, etc.)
- **Communication and exchange of information** with stakeholder(s) is initiated with:
  - LSAs
  - IESOs
  - Enablers
  - Other SMEs
- **Material collected is reviewed and analysed** to ensure proper links with the request are made and expectations are met
- **Relevant material to be used is set aside**
  - Proposed response drafted and reviewed internally
  - External review conducted (if necessary)

RESPONSE PROCESS

Requester is provided with a response to their inquiry(ies)

- **Response is sent to the requester** by email
- **Other individuals are copied** on or informed of the response
- **If necessary:**
  - Further review or research with other authorities can be made and are offered to the requester
  - Information may need to be shared with other stakeholders
- **Response is attached** to the SCoE tracker
- **Feedback process is available** to obtain comments from the requester

REPORTING PROCESS

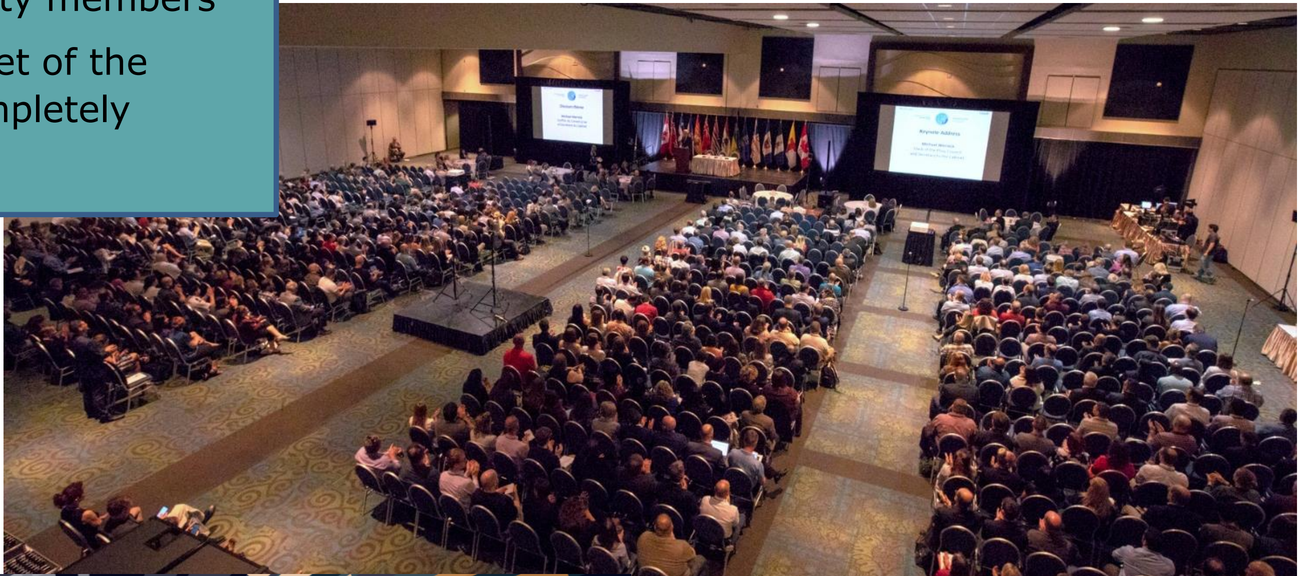
Statistics & trends are available and used to shape future projects and learning events

- **Graphics & reports**
  - **Are created** based on SCoE tracker
  - **Are shared** with the Board of Management
- **High level graphics are shared** through the SCoE Annual Report, distributed to the GC Security Community
- **Statistics and trends are captured in the SCoE work plan** and used to discuss future events and projects based on the SCoE Strategic Plan

Canada

GC Security Summit

- Annual marquis learning event free of charge for the GC Security Community members
- Adapted since onset of the pandemic to a completely virtual experience



2021 GC VIRTUAL SECURITY SUMMIT

Security: Going the Distance

May 17 – 20, 2021

Sommet virtuel sur la sécurité du GC de 2021

La sécurité : le cœur à l'ouvrage

Du 17 au 20 mai 2021

Speaker Series

- Free of charge to members of the Security Centre of Excellence
- Topically timely conference from experts in their field
- Three times a year

Privy Council Office

Recovery and Preparing for the ‘New Normal’

Impacts of Covid-19 on the Security Landscape, looking through a Futures Glass

- Easing of Workplace Restrictions – Making it a Success from the Security Perspective
- Understanding and Managing Security Risks in Virtual Collaboration Tools
- Recovery and Preparing for the ‘New Normal’ - Key Considerations and Priorities for the Security Community
- Fraud - A Perspective for the Security Community

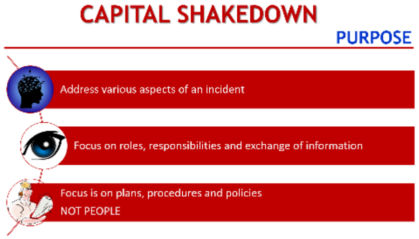
Exercise Metropolitan Mayhem

- Designed and facilitated GC wide exercise resulting in 45 organizations and 500 employees simultaneously participating in TTX within their organization
- Tested BCP knowledge and response to large events impacting the GC
- Tested the Significant Event Information Sharing Protocol
- Scenario involved an earthquake

Other Exercises

Chaos in the City

Capital Shakedown



CAPITAL SHAKEDOWN

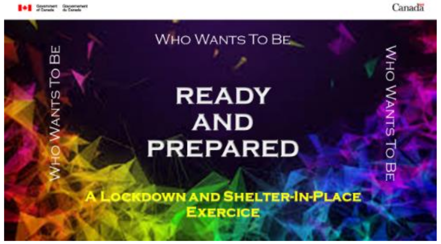
PURPOSE

Address various aspects of an incident

Focus on roles, responsibilities and exchange of information

Focus is on plans, procedures and policies
NOT PEOPLE

Ready and Prepared?



Canadä

WHO WANTS TO BE

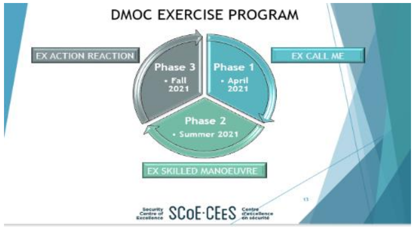
READY
AND
PREPARED

A LOCKDOWN AND SHELTER-IN-PLACE
EXERCICE

WHO WANTS TO BE

WHO WANTS TO BE

DMOC TTX



DMOC EXERCISE PROGRAM

EX ACTION REACTION

Phase 3
- Fall 2021

Phase 1
- April 2021

EX CALL ME

Phase 2
- Summer 2021

EX SKILLED MANOEUVRE

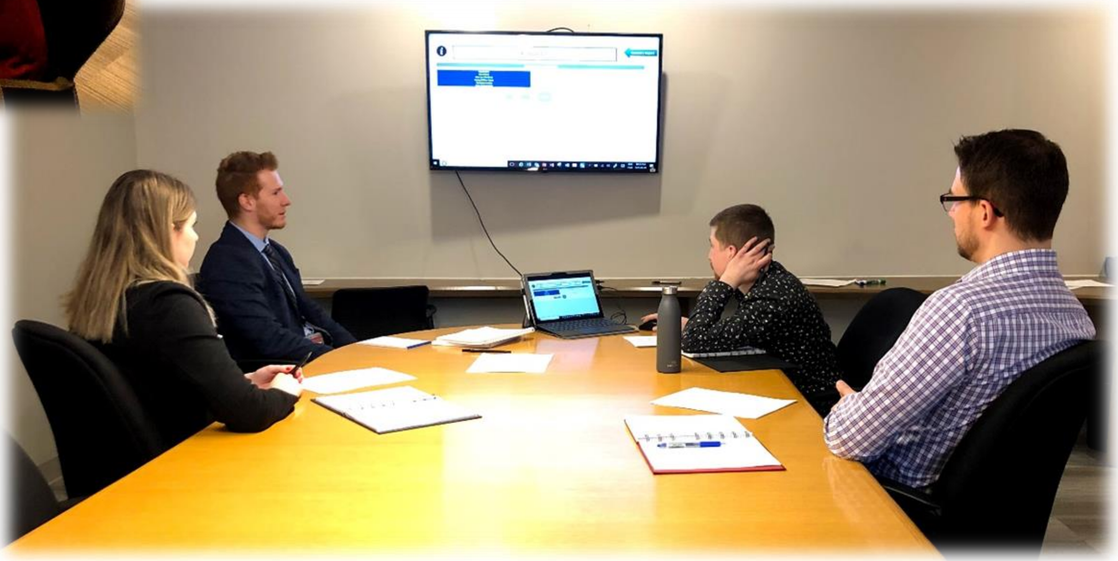
13

Security Centre of Excellence SCoE·CEeS Centre d'excellence en sécurité

SCoE Security Centre of Excellence

Young Security Professionals

- Network of young security professionals
- SCoE chair
- Three activities per year



Discovering new talent

Increasing connections

Sharing knowledge

Innovating & Learning

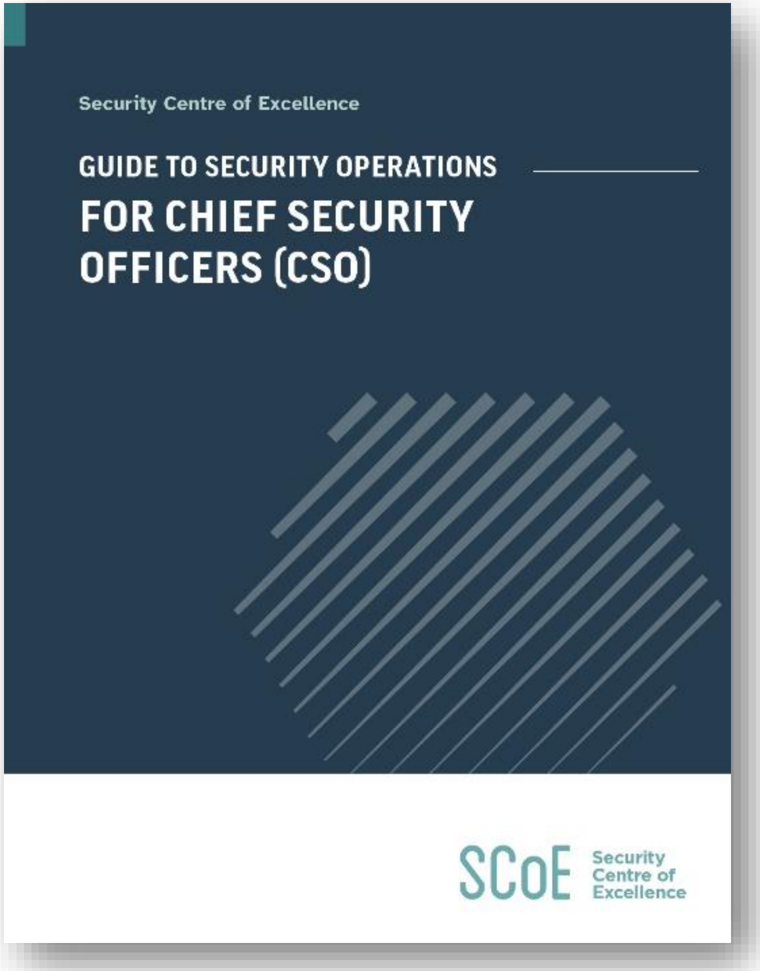
Canada

Recruitment Activities

- Bringing security hiring managers and students in the field together
- Supporting the GC security community to grow
- Facilitating discovery of new talent

Managers find high number of new talents for considerably less time and energy

CSO Guide to Security Operations



Security Centre of Excellence

GUIDE TO SECURITY OPERATIONS

FOR CHIEF SECURITY OFFICERS (CSO)

SCoE Security Centre of Excellence

- Completed the review of the Departmental Security Officer Handbook developed in 2015 to align with new Policy on Government Security
- Conducted interviews with experienced & newly appointed CSOs to obtain advice
- Consulted LSAs and IESO on content

SCoE Security Centre of Excellence

Delivering important community initiatives
In collaboration with partners

Initiate

Identify trends and needs for the GC Security Community based on statistics, inquiries, surveys and GC priorities

Plan

Secure funding, create a plan (activities & timelines) and conceptualize the material needed, aligned with all relevant GC Policies and Guidelines

Execute

Draft material, conduct reviews and pilot with Subject Matter Experts in the GC Security Community and consult with Lead Security Agencies

Monitor

Track project progress and level of effort, ensure timelines are met and milestones are reached

Close

Promote the developed material in committees, at events and on GC Tools, update material and respond to inquiries from the GC Security Community

Canada

SCoE Security Centre of Excellence

ANNEX

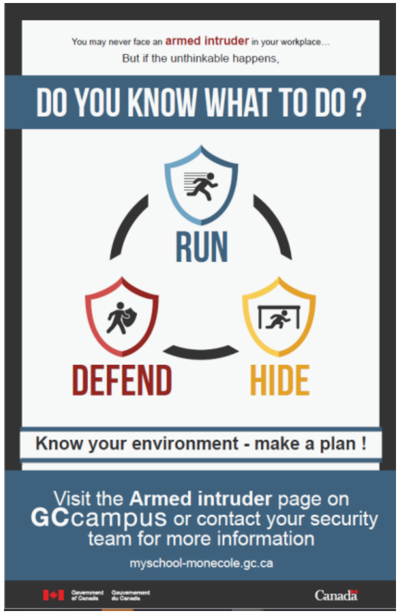
Examples of community initiatives

Canada

SCoE Security Centre of Excellence

GC Armed Intruder Training Package

- Within 6 months of request, delivered a complete training package and briefing material for senior management and employees, including a Canadian GC video
- Plan presented to DSORC where community agreed to use common terminology
- Launched at the 2018 GC Security Summit by the NSIA, a year before new TBS BEET requiring annual exercises
- Included in CSPS security awareness course for all GC employees
- Not made available to the public but shared with other levels of government and academia upon request (Provinces/Municipalities/Universiti es)
- Key partners: RCMP, OCHRO, IRCC, GAC, CRA and Justice



You may never face an **armed intruder** in your workplace...
But if the unthinkable happens,

DO YOU KNOW WHAT TO DO ?

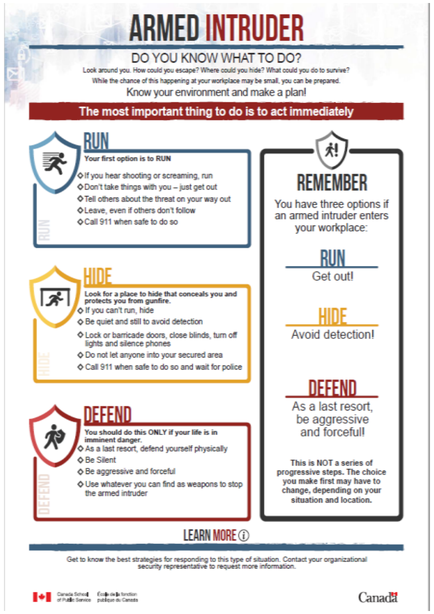
Know your environment - make a plan !

Visit the **Armed intruder** page on **GC**campus or contact your security team for more information

myschool-monecole.gc.ca

Government of Canada Gouvernement du Canada

Canada



ARMED INTRUDER

DO YOU KNOW WHAT TO DO?

Look around you. How could you escape? Where could you hide? What could you do to survive?
While the chance of this happening at your workplace may be small, you can be prepared.
Know your environment and make a plan!

The most important thing to do is to act immediately

RUN

Your first option is to RUN

◇ If you hear shooting or screaming, run
◇ Don't take things with you – just get out
◇ Tell others about the threat on your way out
◇ Leave, even if others don't follow
◇ Call 911 when safe to do so

HIDE

Look for a place to hide that conceals you and protects you from gunfire.

◇ If you can't run, hide
◇ Be quiet and still to avoid detection
◇ Lock or barricade doors, close blinds, turn off lights and silence phones
◇ Do not let anyone into your secured area
◇ Call 911 when safe to do so and wait for police

DEFEND

You should do this ONLY if your life is in imminent danger.

◇ As a last resort, defend yourself physically
◇ Be Silent
◇ Be aggressive and forceful
◇ Use whatever you can find as weapons to stop the armed intruder

REMEMBER

You have three options if an armed intruder enters your workplace:

RUN
Get out!

HIDE
Avoid detection!

DEFEND
As a last resort, be aggressive and forceful!

This is NOT a series of progressive steps. The choice you make first may have to change, depending on your situation and location.

LEARN MORE ⓘ

Get to know the best strategies for responding to this type of situation. Contact your organizational security representative to request more information.

Canada School of Public Service École de la fonction publique du Canada

Canada

INCREASED AWARENESS:
ARMED INTRUDER VIDEO

Canada

Security Infractions Management Toolkit

- Tasked by the Clerk to develop consistent GC approach
- Conducted review of GC practices and presented key findings to DSORC
- Delivered a complete package that covers how to build/change security culture and engage employees of all levels on risks, from on-boarding to corrective measures
- Designed a tool to set frequency of inspections based on risk criteria
- Secured DRDC funding to develop business requirements for an IT CMS
- Elements were included in Safeguarding strategies presented to DMOC and Science and National Security Taskforce
- Key partners: DND, CSIS OCHRO, RCMP, TBS, GAC, ISED

During an inspection, a *Notice of Security Infraction* will be left in your workspace if you have not properly secured sensitive information/assets.

Infractions will be documented and administrative security corrective measures will apply.

SECURITY IS EVERYONE'S RESPONSIBILITY.

Together, we can ensure our sensitive information and assets are securely protected.

Learn more:

(insert contact email here)

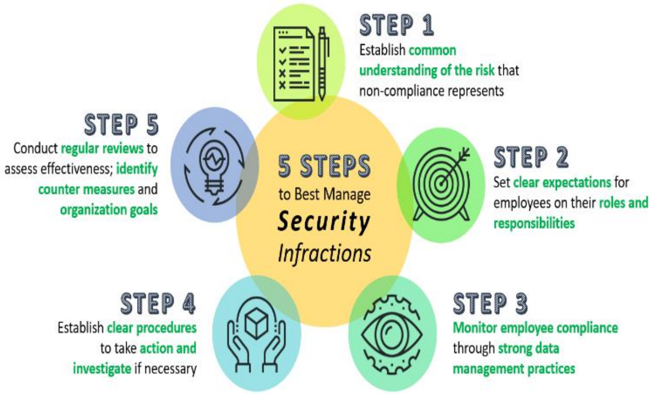
(insert address here)

SECURITY INSPECTIONS

Protecting You and the Organization

We all have a responsibility to protect (insert name of organization here) information and assets. Security inspections help protect the information we hold in trust.

Canada



5 STEPS to Best Manage *Security Infractions*

STEP 1
Establish common understanding of the risk that non-compliance represents

STEP 2
Set clear expectations for employees on their roles and responsibilities

STEP 3
Monitor employee compliance through strong data management practices

STEP 4
Establish clear procedures to take action and investigate if necessary

STEP 5
Conduct regular reviews to assess effectiveness; identify counter measures and organization goals

Management of Security Inspections

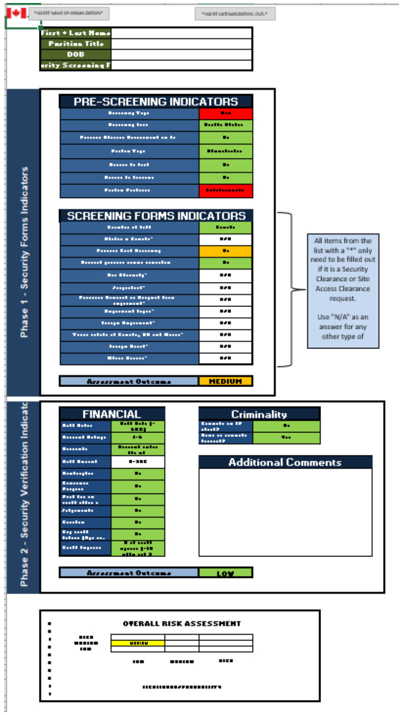
Structured risk assessment methodology to determine security inspection frequency

View Summary Report

Conduct Risk Assessment

Security Screening Toolkit

- Community asked for standardized, adaptable and user-friendly templates they could use to make decision on risk
- Funded by Department of Canadian Heritage (25K)
- Contains over 50 operational supporting documents, templates, guides, SOPs, questionnaires
- Includes a Risk Matrix Excel Tool to assist decision making and drive consistent approach across the community
- Approach and tools allow to expedite the low risk files, focus efforts on the high risk ones and support a timely hiring process while ensuring the risks remain acceptable
- Reviewed by Community of practice and presented to GCSRC
- Shared with CSPS for course development
- Key partners: PCO, PSC, CSPS, CSIS, RCMP, TBS



INSERT NAME OF ORGANIZATION *INSERT CATEGORIZATION LEVEL*

First + Last Name	
Position Title	
DOB	
Security Screening F[illegible]	

Phase 1 - Security Forms Indicators

PRE-SCREENING INDICATORS

SCREENING FORMS INDICATORS

All items from the list with a "*" only need to be filled out if it is a Security Clearance or Site Access Clearance request.

Use "N/A" as an answer for any other type of

Assessment Outcome	MEDIUM

Phase 2 - Security Verification Indicators

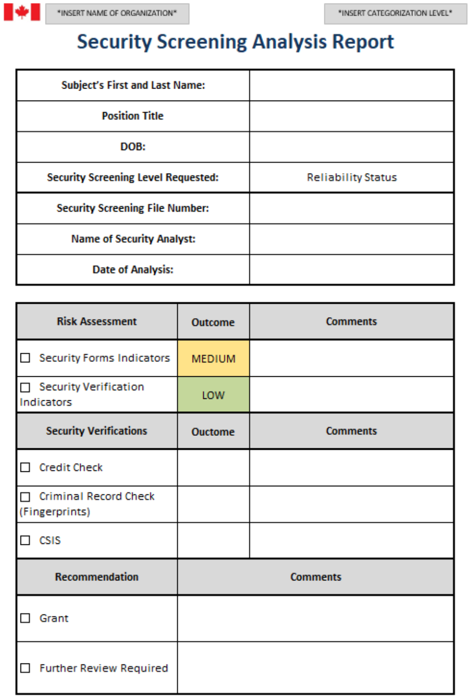
FINANCIAL

Criminality

Additional Comments

Assessment Outcome	LOW

OVERALL RISK ASSESSMENT



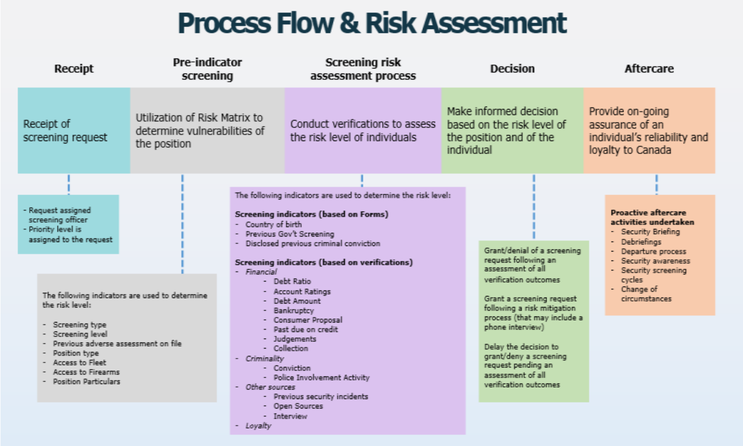
INSERT NAME OF ORGANIZATION *INSERT CATEGORIZATION LEVEL*

Security Screening Analysis Report

Subject's First and Last Name:	
Position Title	
DOB:	
Security Screening Level Requested:	Reliability Status
Security Screening File Number:	
Name of Security Analyst:	
Date of Analysis:	

Risk Assessment	Outcome	Comments
□ Security Forms Indicators	MEDIUM	
□ Security Verification Indicators	LOW	
Security Verifications	**Outcome**	**Comments**
□ Credit Check		
□ Criminal Record Check (Fingerprints)		
□ CSIS		

Recommendation	Comments
□ Grant	
□ Further Review Required	



Process Flow & Risk Assessment

Receipt	Pre-indicator screening	Screening risk assessment process	Decision	Aftercare
Receipt of screening request	Utilization of Risk Matrix to determine vulnerabilities of the position	Conduct verifications to assess the risk level of individuals	Make informed decision based on the risk level of the position and of the individual	Provide on-going assurance of an individual's reliability and loyalty to Canada

Receipt:

- Request assigned screening officer
- Priority level is assigned to the request

Pre-indicator screening:

The following indicators are used to determine the risk level:

- Screening type
- Screening level
- Previous adverse assessment on file
- Position type
- Access to Fleet
- Access to Firearms
- Position Particulars

Screening risk assessment process:

The following indicators are used to determine the risk level:

Screening indicators (based on Forms)

- Country of birth
- Previous Gov't Screening
- Disclosed previous criminal conviction

Screening indicators (based on verifications)

- *Financial*
  - Debt Ratio
  - Account Ratings
  - Debt Amount
  - Bankruptcy
  - Consumer Proposal
  - Past due on credit
  - Judgements
  - Collection
- *Criminality*
  - Conviction
  - Police Involvement Activity
- *Other sources*
  - Previous security incidents
  - Open Sources
  - Interview
- *Loyalty*

Decision:

Grant/denial of a screening request following an assessment of all verification outcomes

Grant a screening request following a risk mitigation process (that may include a phone interview)

Delay the decision to grant/deny a screening request pending an assessment of all verification outcomes

Aftercare:

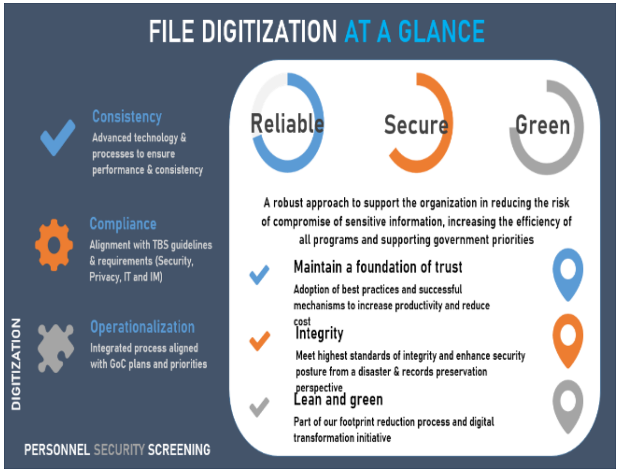
Proactive aftercare activities undertaken

- Security Briefing
- Debriefings
- Departure process
- Security awareness
- Security screening cycles
- Change of circumstances

SCoE Security Centre of Excellence

Digitizing Security Screening Guide

- Greening operations has been an item of interest and a GC priority
- Initiative funded by ECCC (50K)
- Developed a 5 phases guide to assist departments in digitizing their security screening files
- Building on an approach used at the CBSA
- Guide supported by SCoE technical advice as SME
- Multiple organizations on boarded resulting in significant savings, streamlining processes and reducing the footprint
- Allowed security to digitize operations, debunking misconceptions and helping reduce backlogs and transition to remote work
- Organizations have seen the benefit of digitization during the pandemic
- Key partners: CBSA, PSPC



FILE DIGITIZATION AT A GLANCE

DIGITIZATION

Consistency
Advanced technology & processes to ensure performance & consistency

Compliance
Alignment with TBS guidelines & requirements (Security, Privacy, IT and IM)

Operationalization
Integrated process aligned with GoC plans and priorities

Reliable Secure Green

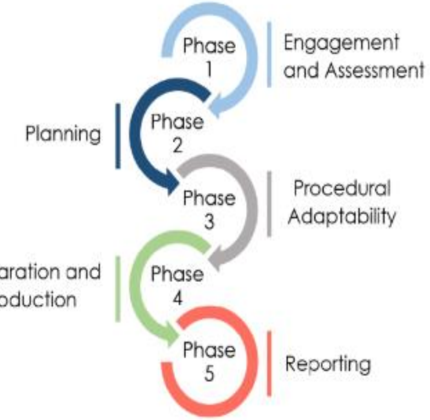
A robust approach to support the organization in reducing the risk of compromise of sensitive information, increasing the efficiency of all programs and supporting government priorities

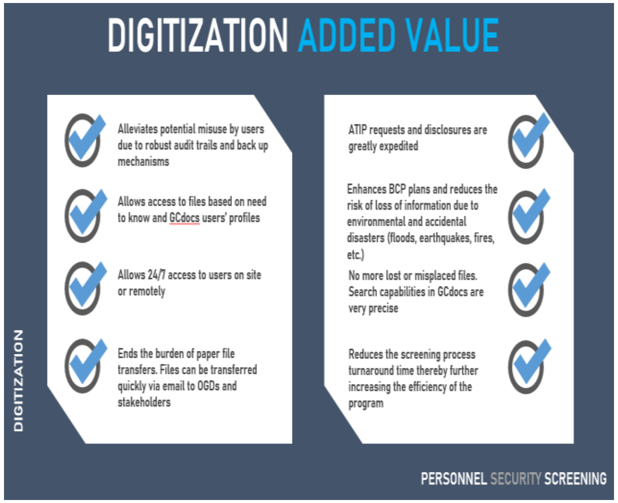
✓ Maintain a foundation of trust
Adoption of best practices and successful mechanisms to increase productivity and reduce cost

✓ Integrity
Meet highest standards of integrity and enhance security posture from a disaster & records preservation perspective

✓ Lean and green
Part of our footprint reduction process and digital transformation initiative

PERSONNEL SECURITY SCREENING





DIGITIZATION ADDED VALUE

DIGITIZATION

✓ Alleviates potential misuse by users due to robust audit trails and back up mechanisms

✓ Allows access to files based on need to know and GCdocs users' profiles

✓ Allows 24/7 access to users on site or remotely

✓ Ends the burden of paper file transfers. Files can be transferred quickly via email to OGDs and stakeholders

ATIP requests and disclosures are greatly expedited ✓

Enhances BCP plans and reduces the risk of loss of information due to environmental and accidental disasters (floods, earthquakes, fires, etc.) ✓

No more lost or misplaced files. Search capabilities in GCdocs are very precise ✓

Reduces the screening process turnaround time thereby further increasing the efficiency of the program ✓

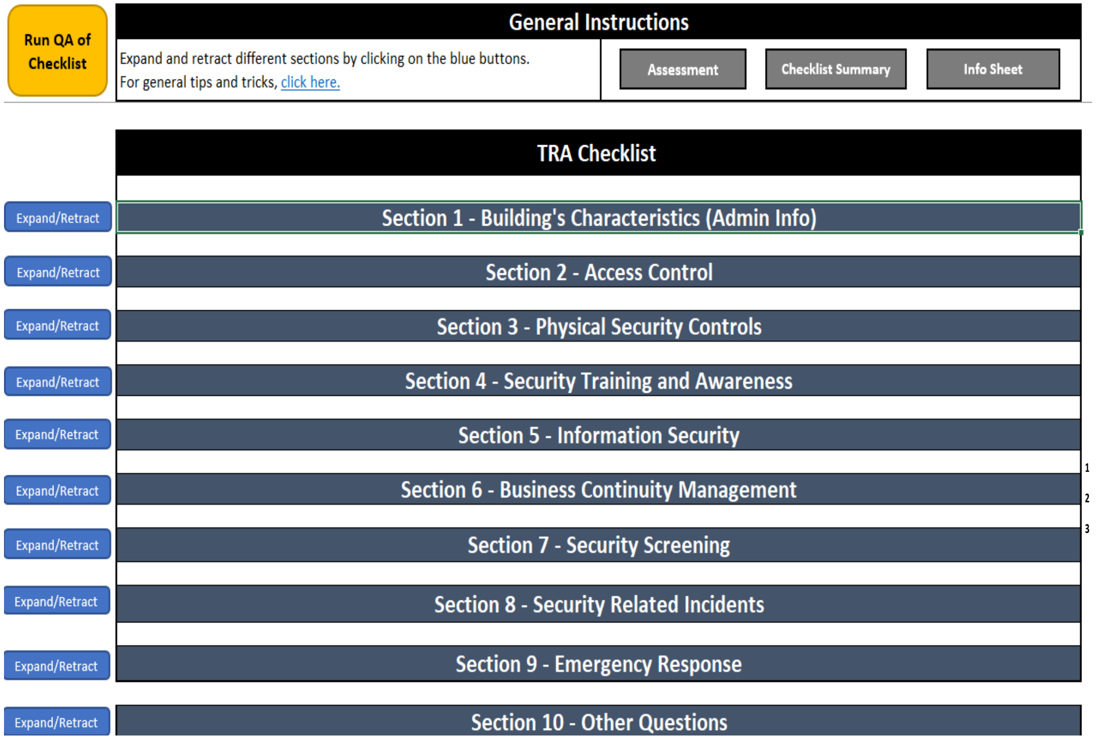
PERSONNEL SECURITY SCREENING

Canada

Threat and Risk Assessment Toolkit

- Funded by Heritage (25K), piloted at PCO. Includes operational supporting documents, SOPs and User friendly Excel TRA Assessment tool
- Presented to community of practice and scheduled for GCSRC in April 2021
- Key partners: CBSA, PCA, PCO + LSAs (RCMP & PSPC)

Automated Tool

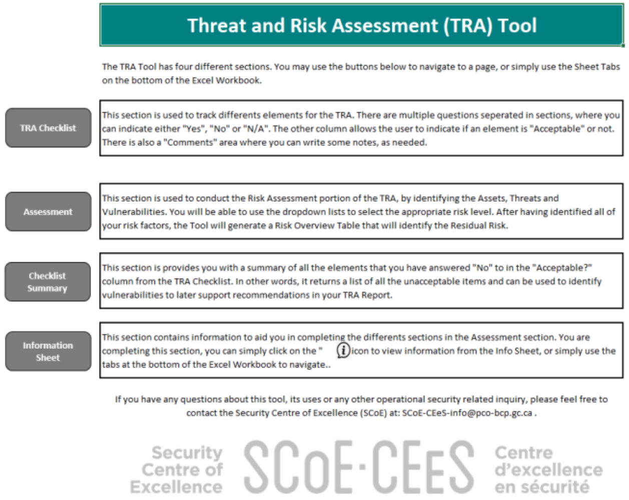


General Instructions

Expand and retract different sections by clicking on the blue buttons.
For general tips and tricks, click here.

TRA Checklist

- Section 1 - Building's Characteristics (Admin Info)
- Section 2 - Access Control
- Section 3 - Physical Security Controls
- Section 4 - Security Training and Awareness
- Section 5 - Information Security
- Section 6 - Business Continuity Management
- Section 7 - Security Screening
- Section 8 - Security Related Incidents
- Section 9 - Emergency Response
- Section 10 - Other Questions



Threat and Risk Assessment (TRA) Tool

The TRA Tool has four different sections. You may use the buttons below to navigate to a page, or simply use the Sheet Tabs on the bottom of the Excel Workbook.

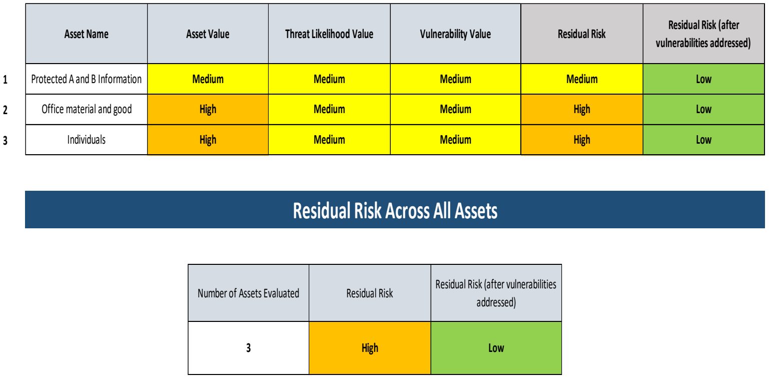
This section is used to track differents elements for the TRA. There are multiple questions seperated in sections, where you can indicate either "Yes", "No" or "N/A". The other column allows the user to indicate if an element is "Acceptable" or not. There is also a "Comments" area where you can write some notes, as needed.

This section is used to conduct the Risk Assessment portion of the TRA, by identifying the Assets, Threats and Vulnerabilities. You will be able to use the dropdown lists to select the appropriate risk level. After having identified all of your risk factors, the Tool will generate a Risk Overview Table that will identify the Residual Risk.

This section is provides you with a summary of all the elements that you have answered "No" to in the "Acceptable?" column from the TRA Checklist. In other words, it returns a list of all the unacceptable items and can be used to identify vulnerabilities to later support recommendations in your TRA Report.

This section contains information to aid you in completing the differents sections in the Assessment section. You are completing this section, you can simply click on the " ⓘ icon to view information from the Info Sheet, or simply use the tabs at the bottom of the Excel Workbook to navigate..

If you have any questions about this tool, its uses or any other operational security related inquiry, please feel free to contact the Security Centre of Excellence (SCoE) at: SCoE-CEeS-info@pco-bcp.gc.ca .



	Asset Name	Asset Value	Threat Likelihood Value	Vulnerability Value	Residual Risk	Residual Risk (after vulnerabilities addressed)
1	Protected A and B Information	Medium	Medium	Medium	Medium	Low
2	Office material and good	High	Medium	Medium	High	Low
3	Individuals	High	Medium	Medium	High	Low

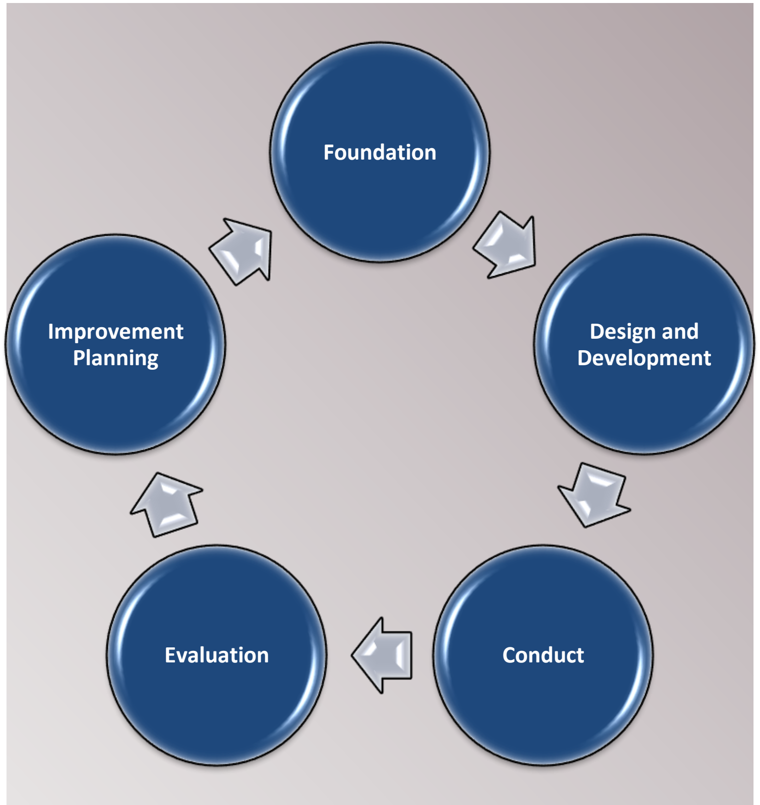
Residual Risk Across All Assets

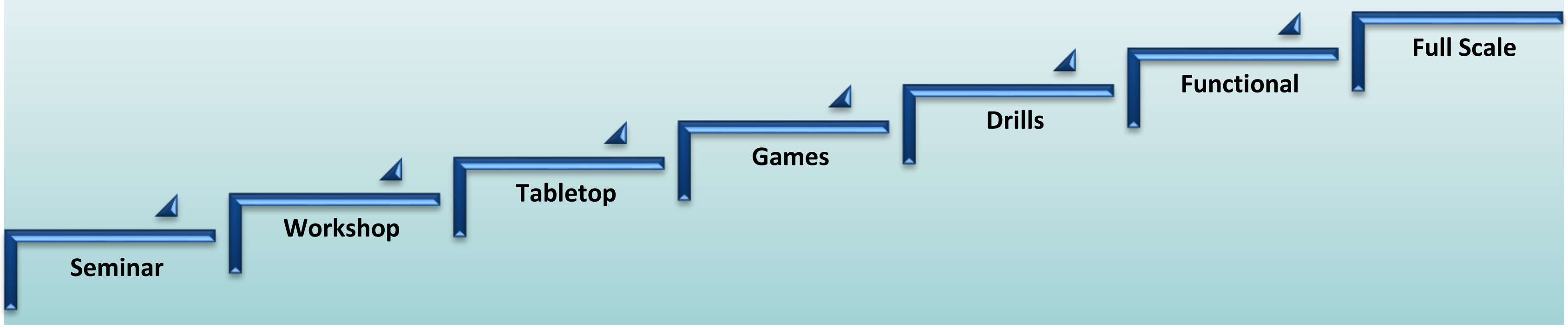
Number of Assets Evaluated	Residual Risk	Residual Risk (after vulnerabilities addressed)
3	High	Low

SCoE Security Centre of Excellence

Exercise Planning Toolkit

- Support for exercise development.
- Addresses key exercise development challenges:
  - How do I obtain approval
  - What if I lack exercise experience
  - Where do I seek expertise
  - How do I get buy-in from other GC organizations
  - How do I manage my time to meet planning deadlines
  - Which scenario is best for me
  - What are exercise safety requirements
  - Why do I need to evaluate the exercise


Foundation
Design and Development
Conduct
Evaluation
Improvement Planning


Seminar
Workshop
Tabletop
Games
Drills
Functional
Full Scale