

**Spring Knowledge Café Presentation:
Security Centre of Excellence – Building Resilience**

June 12th, 2025

Jean-François Savard, CD, MA, CPP, CISSP, CBCP, CFE

Background and context I

- The SCoE, formerly known as the DSO Centre for Development (CfD), has been in operation since 2012
- When its mandate was renewed in 2017, the then National Security and Intelligence Advisor (NSIA) to the Prime Minister endorsed the pursuit of the Centre's operations for 5 additional years with the following expectations:
 - Transition to a GC Security Centre of Excellence
 - Establish a governance to allow input from the entire Government of Canada's security community into the Centre's orientations and activities
- 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 16,000 security officials
 - NSIA's role as the Champion of Government Security
 - PCO's Lead Security Agency(LSA)'s 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

Background and context II

- The governance of the SCoE needed to reflect this fact so a two-tiered GC Security Community oversight structure was created:
 - Board of Directors – PCO, TBS, Public Safety and rotating member from LSAs – provide overarching priorities and strategy
 - Board of Management (BoM) – six CSOs from two large, two medium and two small departments/agencies – provides hands-on oversight of the SCo's operations and planning
- The Centre works on Five-Year Plans that are recommended by the BoM and approved by the BoD on behalf of the GC Security Community that funds its operations
- Annual Reports are sent out to the GC Community outlining its activities
- The SCoE has three mutually-supporting values:
 - Accountability
 - Collaboration
 - Excellence

Excellence in Security: #Ready and Prepared

Strategic Objectives

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



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;

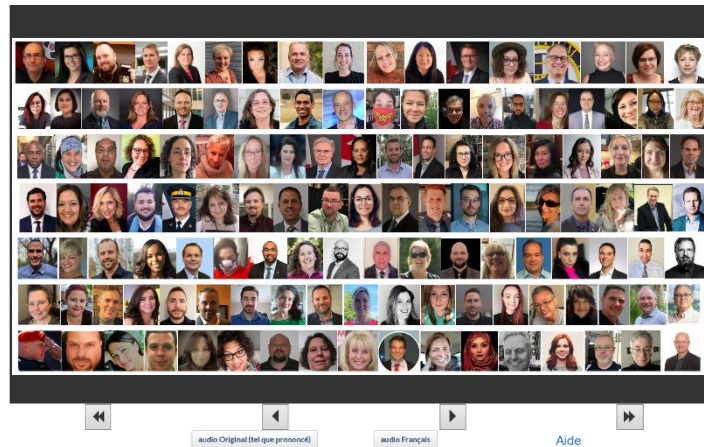
Knowledge

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

Stronger together

Connecting the community

Government of Canada Virtual Security Summit 2020



audio Original (tel que prononcé) | audio Français | Aide



Government of Canada / Gouvernement du Canada | GCollab | GWiki | GMessage (Pilot)

Home | Communities | This Site | Groups | Members | Career | More

Security Centre of Excellence / Centre d'excellence en sécurité

Owner: SCoE-CEES | Group members: 887

Activity | Discussion | Files | Events | More

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 open 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 GCollab. 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 future such as this help facilitate the sharing of information, ideas, and updates to reinforce those vital links.

Join the SCoE mailing list to be informed about hot topics in security, upcoming training 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 guide on GCollab: Security Shopping Tools. Your CSO/CSOC can send us the names and email addresses of their customers who require access to SCoE.

Quoi de neuf ?

NOUVEAU

Le CCoE a récemment développé et publié un nouveau guide sur GCollab: L'achat de produits de sécurité. Votre CSO/CSOC peut nous envoyer les noms et les adresses électroniques de leurs clients qui ont besoin d'accéder à SCoE.

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.

For quick access to knowledge sharing, subscribe here.

Security Centre of Excellence | SCoE-CEES | Centre d'excellence en sécurité

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 GCollab, our knowledge sharing and community networking hub. Stay in the know with future bulletins by subscribing here.

- PSF
- HC
- CCI
- GA

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!

What We Do

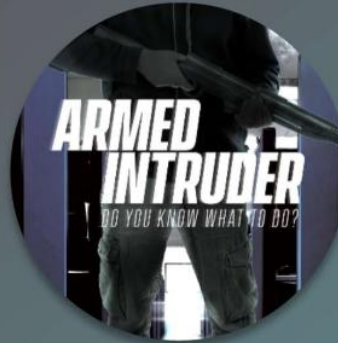
**Young Security
Professionals Network**



**GC Security
Summit**



**Community Driven
Projects**



**Capacity
Building**



**Advice and
Guidance**



**SCoE
Speakers Series**



**Sharing Best
Practices**



**Exercising the
Security Community**

Services Offered

- **Advice and Guidance**
 - Most used service at SCoE (close to 2000 requests in 2024-25)
 - Confidential service, analysts do not report back to central agencies
 - Usual turnaround within 24 hrs, but up to five days, or sometimes longer, if more complex issues

- **Tool Kits**
 - Toolkits cover a variety of issues including security screening, security in contracting, travel security, security awareness, physical security, security sweeps, etc...

- **Analysis**
 - Detailed analyses of issues important to the GC security Community such a:
 - Professionalization Study and Competency Profiles up to and including for CSOs
 - Demographic Study
 - Leveraging Intelligence for Chief Security Officers Study
 - Needs Analysis

Services Offered

- **Networks**

- Young Professionals' Network
- Managers' Network

- **Mentoring Program**

- Over 100 matches between mentors and mentees in 2024-25
- Looking at launching an executive coaching service for CSOs/DCSOs in the autumn

- **Recruiting and Staffing**

- Collaborations with local educational institutions to assist clients in recruiting drives
- Collective processes held on behalf of the GC Security Community
- (currently running S-03 and AS-05 processes, with one planned for EX-01s next)

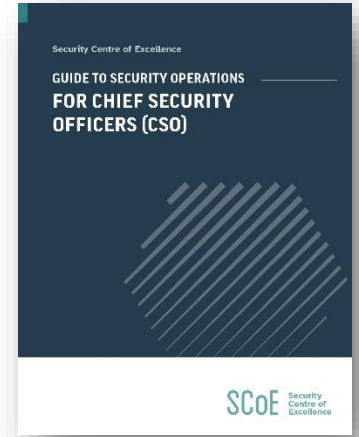
- **Events**

- Quarterly Speakers Series Events
- Annual GC Security Summit

- **Exercises**

- Annual CSO Exercises
- Tailored Tabletop Exercises (TTXs) developed for clients to run themselves or with the assistance of SCoE staff
- Generic TTXs delivered to client's organizations drawn from library of exercise types
- Facilitated discussions on various topics

For the whole community



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

Impact on GC Security Community

- In delivering on its strategic objectives, the Centre looks to achieve the following outcomes for the GC Security Community:
 - **Resilience:**
 - The ability of the GC security community to adjust easily to change and to recover rapidly from incidents or events. The ability to maintain sustained efforts during emergencies;
 - **Readiness:**
 - The state in which the GC security community is prepared to respond quickly and effectively to events, incidents, and issues;
 - **A capable workforce:**
 - Skilled, professional and recognized GC security functional specialists;
 - **Risk mitigation:**
 - Managed approach to reduce the impact, severity and/or probability of occurrence of known risks affecting the GC and its operations.

Background Slides

GC Security Summit

- Annual marquee learning event free of charge for the GC Security Community members
- Adapted since onset of the pandemic to a hybrid format



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

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



Privy Council Office



Recovery and Preparing for the 'New Normal'

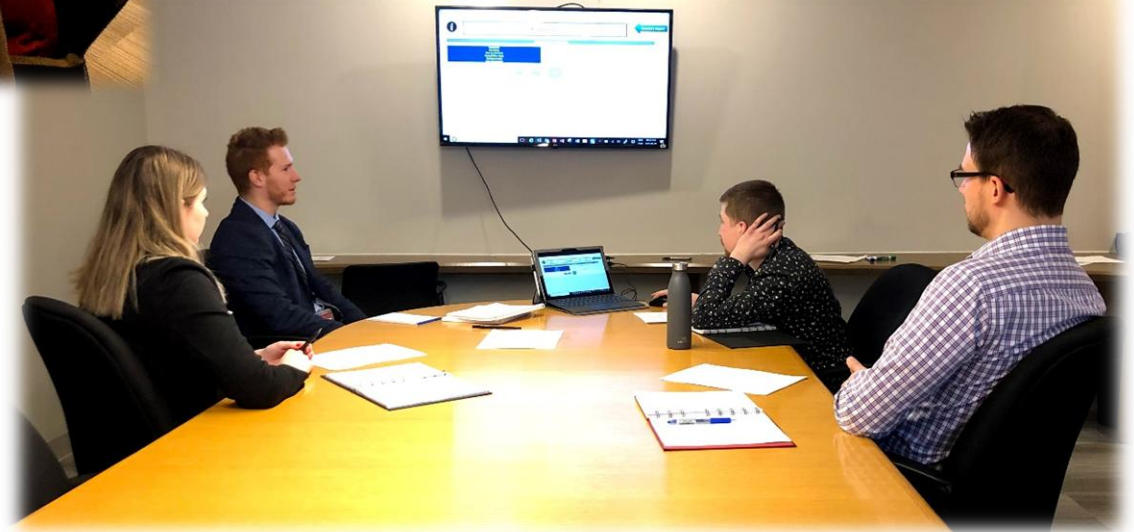
- Easing of Workplace Restrictions – Making it a Success from the Security Perspective
- Understanding and Managing Security Risks in Virtual Collaboration Tools
- Recovery and Preparing for the 'New Normal' - Key Considerations and Priorities for the Security Community
- Fraud - A Perspective for the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

Young Security Professionals



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

*Discovering new talent
Increasing connections
Sharing knowledge
Innovating & Learning*



Recruitment Activities

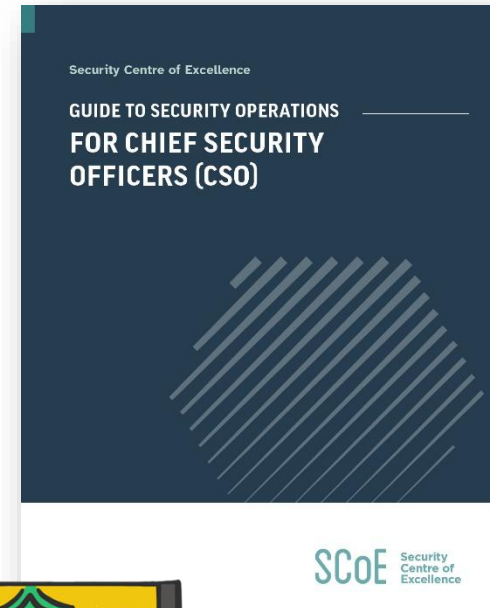
- Bringing security hiring managers and students in the field together
- Supporting the GC security community to grow
- Facilitating discovery of new talent



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

CSO Guide to Security Operations

- 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
- Text in both official languages finalized in March 2021 and expected to be published in Q1 2021-22
- Promotion of this reference material will be done at various fora
- Proposal for CSO orientation and mentoring sessions pending



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 resources
 - ▶ 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

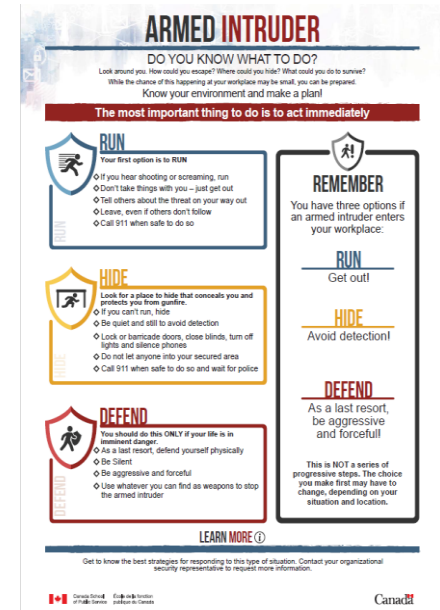
REPORTING PROCESS

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

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 CSPA 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/Universities)
- Key partners: RCMP, OCHRO, IRCC, GAC, CRA and Justice




INCREASED AWARENESS: ARMED INTRUDER VIDEO




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
- Design 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.



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

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
- Build on 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

Consistency
Advanced technology & processes to ensure performance & consistency

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

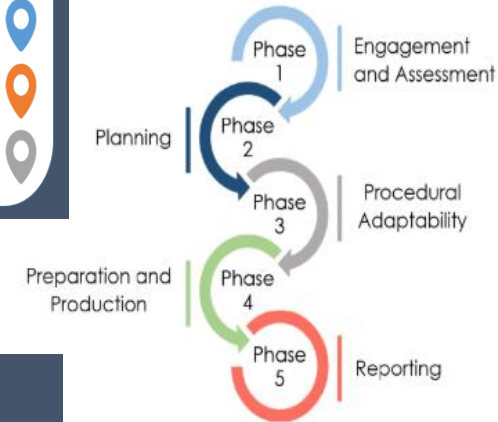
Operationalization
Integrated process aligned with GoC plans and priorities

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

DIGITIZATION PERSONNEL SECURITY SCREENING



DIGITIZATION ADDED VALUE

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

DIGITIZATION PERSONNEL SECURITY SCREENING

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
- Key partners: CBSA, PCA, PCO + LSAs (RCMP & PSPC)

Automated Tool

Run QA of Checklist

General Instructions

Expand and retract different sections by clicking on the blue buttons.
For general tips and tricks, [click here](#).

Assessment

Checklist Summary

Info Sheet

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

TRA Checklist

This section is used to track different elements for the TRA. There are multiple questions separated 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.

Assessment

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.

Checklist Summary

This section 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.

Information Sheet

This section contains information to aid you in completing the different sections in the Assessment sheet. 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)
Protected A and B Information	Medium	Medium	Medium	Medium	Low
Office material and good	High	Medium	Medium	High	Low
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

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?

WHO WANTS TO BE
READY AND PREPARED
A LOCKDOWN AND SHELTER-IN-PLACE EXERCISE

DMOC TTX

