Reflections of a former DND/CAF Chief Security Officer (CSO)

BGen (Ret’d) Andre Demers OMM, MSC, CD

27 March 2025

Agenda

- Introduction (and caveat)
- DND/CAF “101”
- Director General Defence Security (DGDS)
- BCM Realignment Efforts
  - Business Impact Analysis, Leadership buy-in and “keep calm and carry on”
  - Transformation “under contact”
- Some key take aways
- Discussion/Questions

DND/CAF “101”

The Canadian Armed Forces (CAF) are the unified military forces of Canada, consisting of land, sea, and air components known as the Canadian Army, Royal Canadian Navy, and Royal Canadian Air Force (and other key elements)

Components

- Regular Force: Full-time professional military personnel
- Reserve Force: Part-time personnel
- Canadian Rangers

The CAF is responsible for eight core missions (of note):

- Detecting and defending against threats to Canada
- Defending North America in partnership with the United States
- Contributing to NATO and coalition efforts globally
- Provide assistance to civil authorities in Canada (including Search and Rescue (SAR))

FE

FG

Recover

DND/CAF DGDS & CSO Mandate

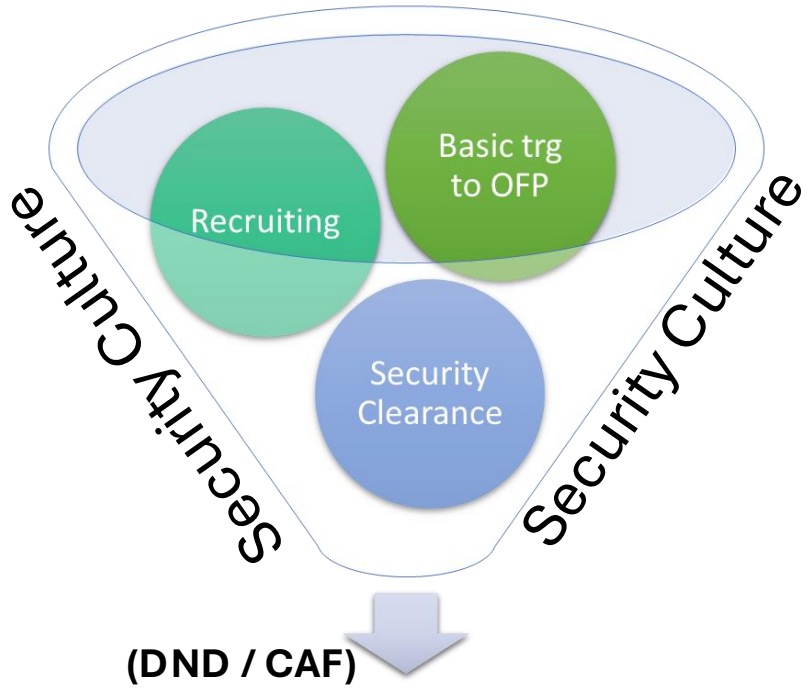
DGDS Mandate:

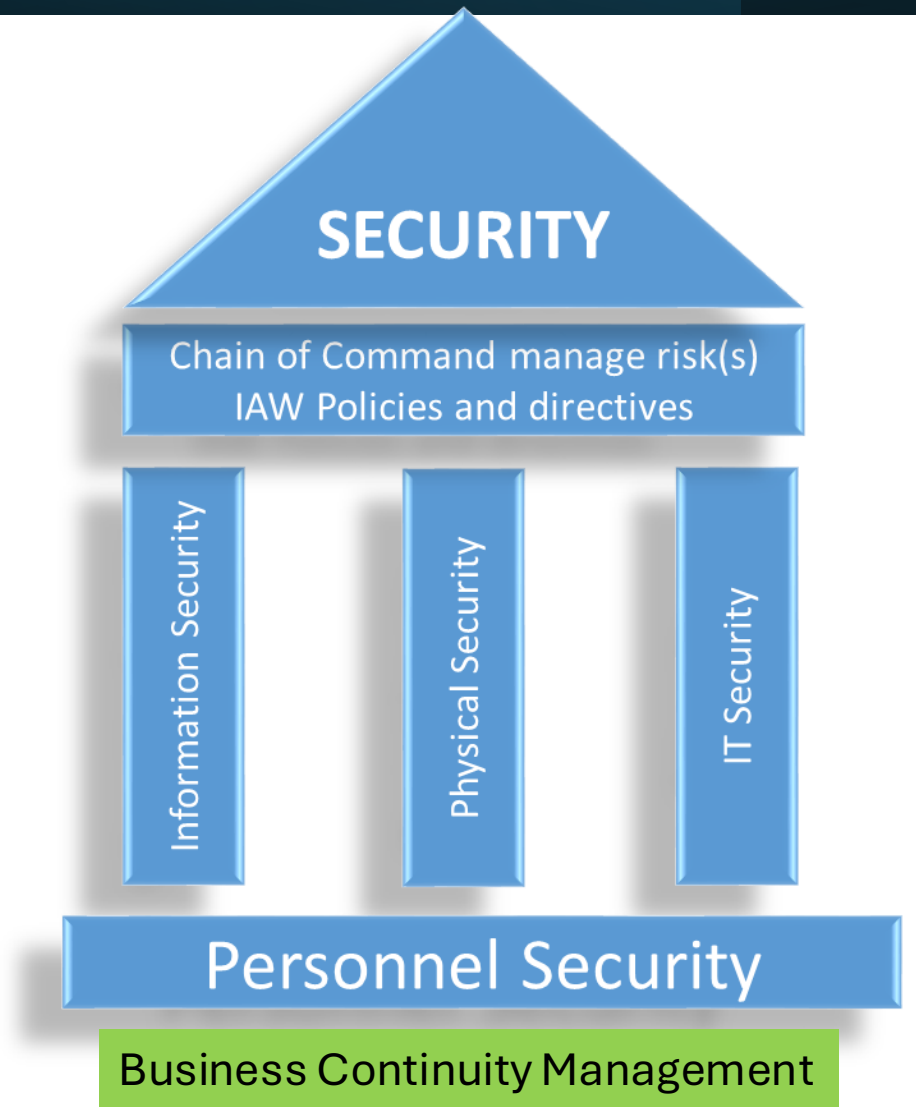
To protect, promote and support security in DND/CAF activities and operations by executing its functional authority leadership and implementing effective security programs.

Overall Responsibilities

- **Planning** - Departmental Security Plan (DSP)
- **Governance** – accountability, delegations, roles & responsibilities for employees with security responsibilities
- **Managing Security Risks** – systematic management of security risks; formal acceptance of residual risks as defined in DSP
- **Monitoring and Oversight** – effectiveness and currency of security controls; corrective action when necessary
- **Performance Measurement and Evaluation** – quality assurance programs to verify that security controls most efficiently and effectively meet departmental security requirements
- **Government-wide Support** – reporting security incidents, issues or concerns to central agencies & service providers; implementing mitigation advice from lead security agencies and reporting on actions taken

DGDS


Recruiting
Basic trg to OFP
Security Clearance
Security Culture
Security Culture
(DND / CAF)
Operational output


SECURITY
Chain of Command manage risk(s) IAW Policies and directives
Information Security
Physical Security
IT Security
Personnel Security
Business Continuity Management


SECURITY SCREENING
IT SECURITY
PHYSICAL SECURITY
BUSINESS CONTINUITY MANAGEMENT
IM SECURITY
SECURITY IN CONTRACTS
SECURITY EVENT MANAGEMENT
SECURITY AWARENESS AND TRAINING

DND/CAF DGDS Team

Director Security Liaison & Corporate Affairs (Civ Director)

- Departmental Security Plan (DSP)
- L0 Business Continuity Program (BCM)
- Senior Security Advisory Committee (SSAC)
- Security Information Exchange Network (SIXNET)
- Corporate Reporting
- Management Accountability Framework (MAF)
- Finance/Admin Issues Management, Accommodations, HR

Director Defence Security Operations (Military Col, +6 RDSOs)

- Physical Security / Security Risk Management
- Industrial Security (IS)
- Information Systems Security (ISS)
- Security Event Management (SEM)
- Travel and Contact Security Program (TCS)
- Special Programs Coordination Office (SPCO)

Director Security Policy, Training & Awareness (Military Col)

- Policy (PGS Reset + NDSODs update)
- Security Awareness and Training
- Security Performance & Evaluation
- MOU monitoring/advice related to security
- Policy alignment with GC and allies

Director Personnel Security & Identity Management (CIV Director)

- Personnel security screening
  - Resolution of doubt
- National Defence Identity Programme
  - Biometrics (Fingerprinting of CAF members)
  - Operational ID Card production
  - Veteran's Service Card
- Personnel Security Capabilities Management
  - Project Sentinel
  - Quality assurance

DGDS – Battle Space Framework

DPSIM

DDSO, DDSPTA, DSLCA

Deep

Common standard for security in line with domestic and allies

Security culture driven by Chain of Command

Quality Assurance

Adapting to changes in the COE in order to be postured for the FSE

Transformation under contact

- AI/Big Data/Analytics/Social Media and OSINT Monitoring
- Develop a Personnel Security Career path (including required training)
- Enduring evolution of process

ICAM

Policy Integration GoC and OGD

Close

Operational output (Vital ground)

RS

SC

- Process Overhaul
- Integrate SSE/OP Generation
- IT upgrade (constant)
- Policy review (NDSOD Chap 4)

Operational output (Vital ground)

ID Mgt

Biometrics collection

Temp ID Mgt

DND/CAF Policy Integration

NDSOD

BCP

Risk Mgt

Rear

Resolution of doubt

ID Mgt

- Relationship with key domestic and allies
- Staff recruiting and retention
- Legal review (as required)
- Auditing (internal and independent)
- GBA+

Vet Card

Biometrics DB

Corporate Reporting

Trg and Awareness

BCM

Key Terrain: Human Resources
Battle Winning Idea: Robust Quality Assurance

Key Terrain: RDSOs and NDSODs
Battle Winning Idea: Chain of Command manage risk

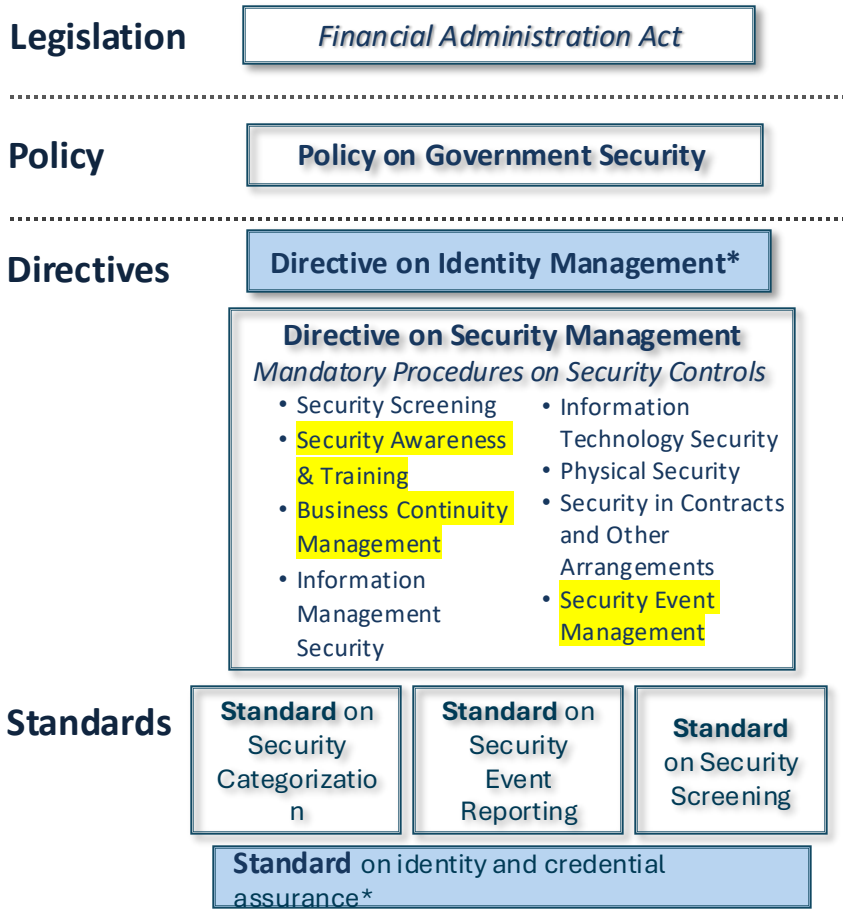
Context of BCM Efforts

- 2015: scientific methodology developed for prioritization of NCR critical services
- October 2016: Public Safety Audit of the Business Continuity Planning Program
- July 2019: Amendments to *Policy on Government Security* and the *Directive on Security Management* come into effect
- October 2019: Public Safety releases A Government of Canada Guide for Developing a Business Continuity Management Program
- COVID 19 (Critical Services List)
- Restructuring of DGDS/DSLCA
  - Staff turnover
  - Restructure resulted in team of three being reduced to one BCP Analyst

Policy instruments

- Policy on Government Security: Annex A: Security Controls
  - Business continuity management is conducted systematically and comprehensively to provide reasonable assurance that in the event of a disruption, the department can maintain an acceptable level of delivery of critical services and activities, and can achieve the timely recovery of other services and activities.
- Directive on Security Management (July 2019)
  - Authorities
  - Objs and expected results
  - Requirements
  - Annex D: Mandatory Procedures for Business Continuity Management Control
- DND BCM Requirements: NDSODs Chapter 10
  - Strategic-level Governance structure
  - BIA
  - Training and exercises
  - Roles and Responsibilities of SJS, DGDS, respective L1s

PGS Architecture



Note: *Standard on Security Screening* not included in the reset exercise

*Highlighted in blue: Instruments to be transitioned to Digital Policy (effective date TBD)

Policy sets out:

- Deputy head responsibility for eight security controls
- Requirement to appoint Chief Security Officer
- Integrated and enterprise approach to security management in a shared risk/operating environment

Directive on Security Management:

- CSO responsibilities for security controls
- Describes mandatory procedures for security controls
- Roles and responsibilities for senior officials, security practitioners and employees

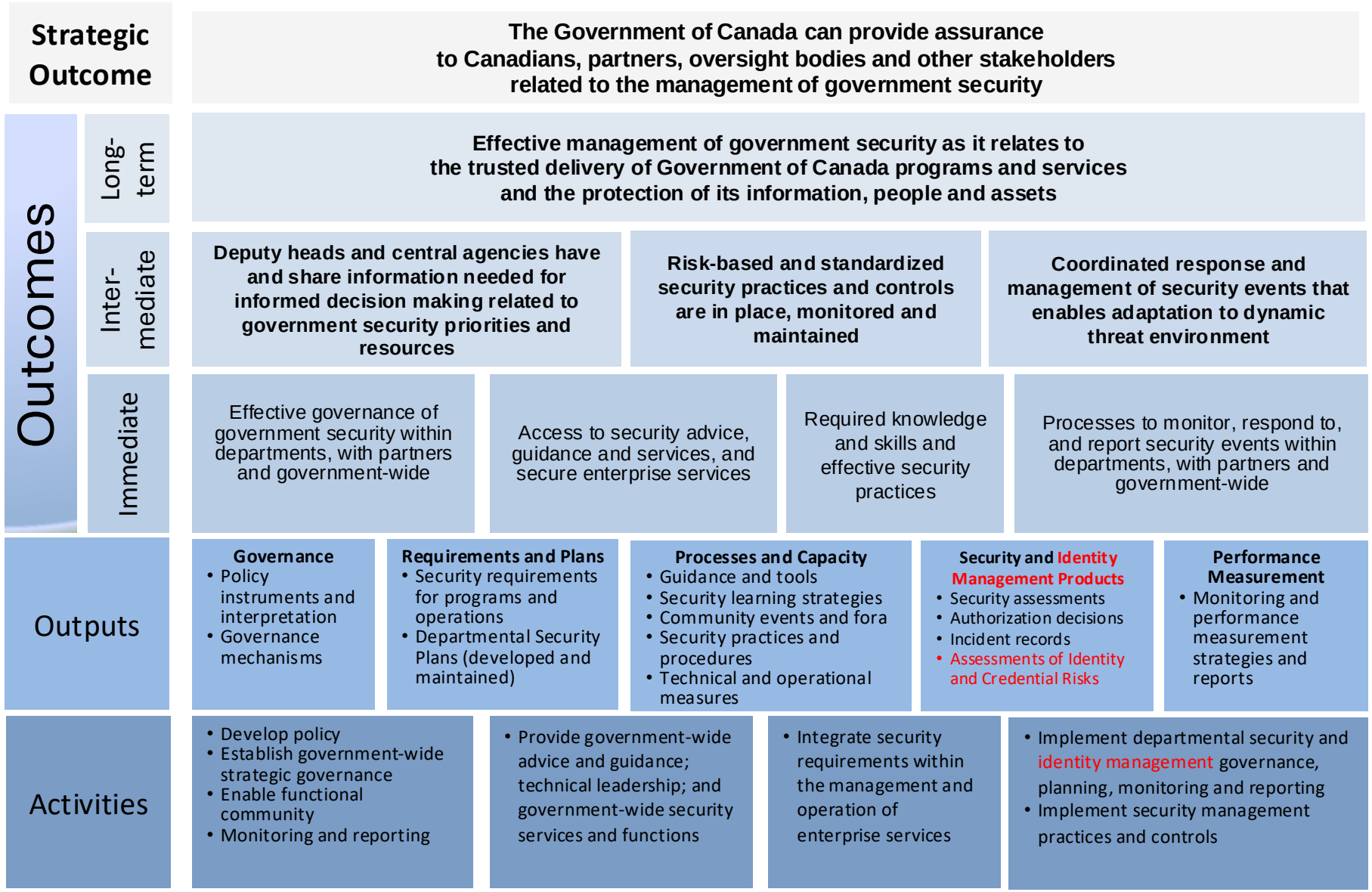
Standards:

- Provide detailed operational guidance and requirements
- Event Coordination roles and responsibilities

Related guidance and tools:

- Provide departments and practitioners with prescriptive support (with assistance of LSAs)

PGS Logic Model



BCM SWOT Analysis

Strengths

- Exec forum (ISC-BCP, BCP-WG) access CDS/DM/VCDS
- Existing BCM program good foundation/starting point for improvements
- Visibility at higher level (recognized as a departmental corporate risk)

Weaknesses

- Insufficient staff/resources
- L1/L2 Organisation with L0 Functional Authority (CSO role) – SJS/CorpSec/CDS/DM not sufficiently involved in BCM process
- Absence of KPIs

Opportunities

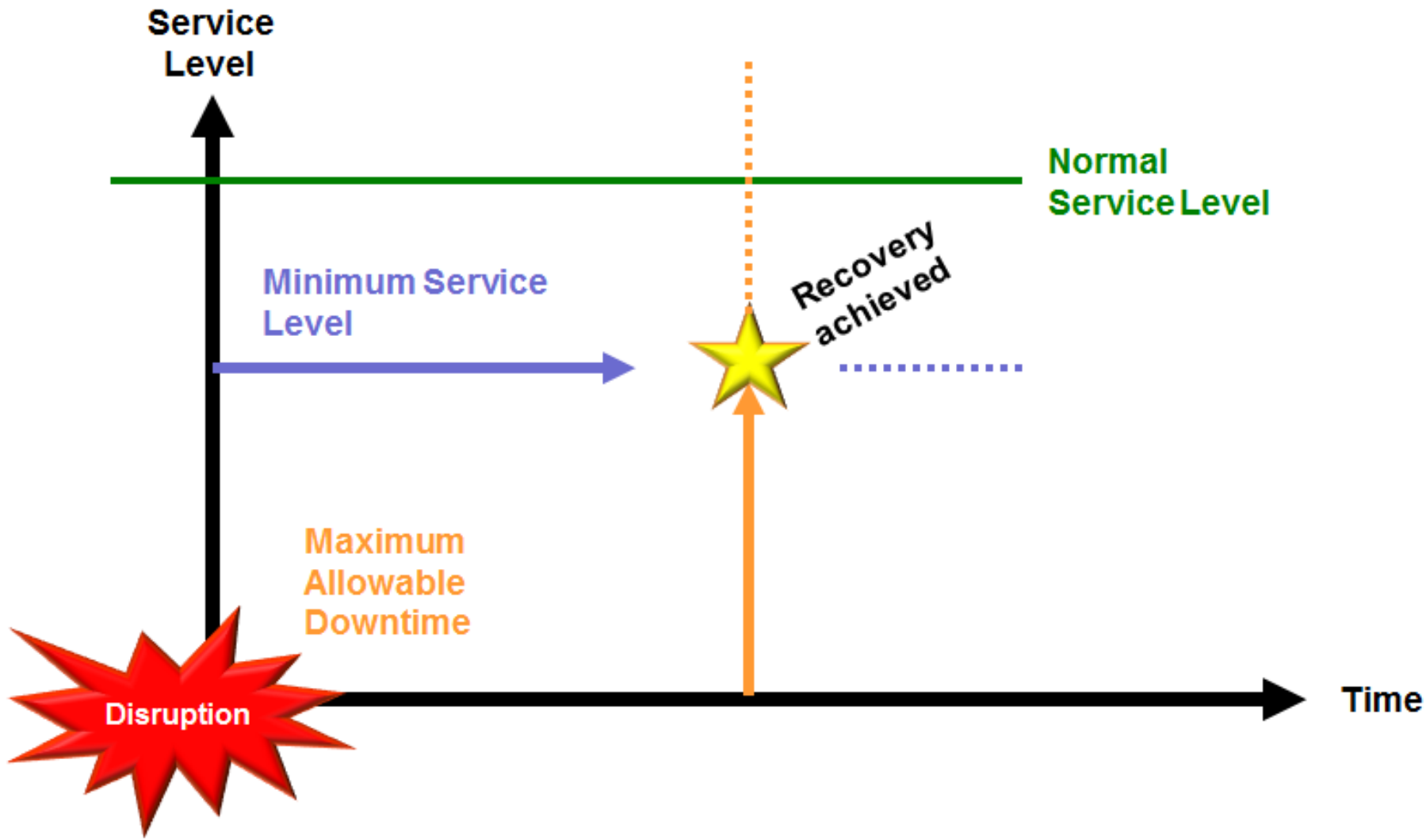
- ADM(RS) Audit
- Public Safety Audit
- COVID-19 pandemic visibility
- BCP expanding business
- Community practice

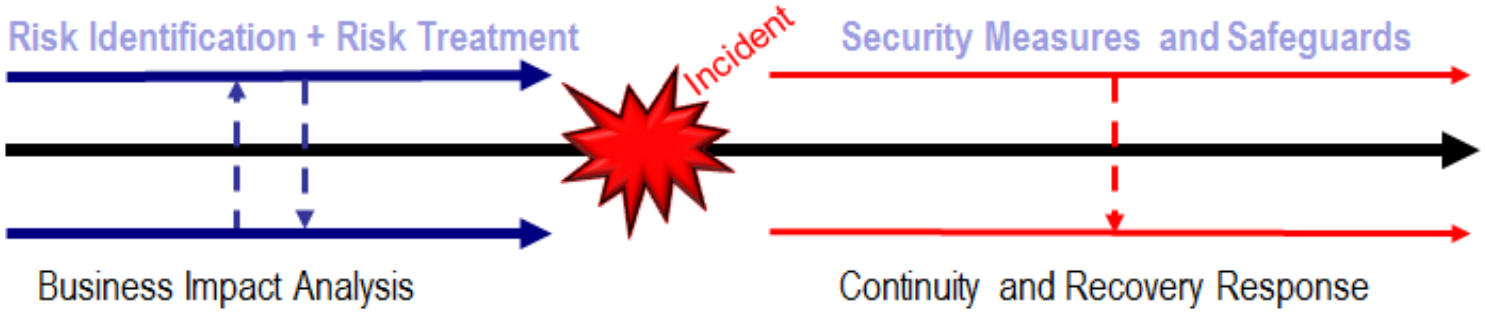
Threats

- DND successful at BCM without program
- Program's credibility
- TBS reporting requirement
- Competing departmental priorities
- Uncoordinated and unplanned resources requirement in moment of crisis/event

BCM Mission Analysis

- To obtain DGDS guidance and approval on the Senior Business Continuity Planning Analyst’s understanding of her mandate, priorities, key deliverables, milestones, and methodology in the overhaul of the Business Continuity Management program for DND/CAF.


Service Level
Normal Service Level
Minimum Service Level
Recovery achieved
Maximum Allowable Downtime
Disruption
Time



Threat and Risk Treatment to Identify Risks

If the risk is acceptable, it needs no further treatment.
If the level of risk is determined to be unacceptable, then apply risk treatment:

Reduce – Avoid – Transfer – Share

Risk Evaluation

Determining if risk is acceptable or not, determining the appropriate treatment and mitigation

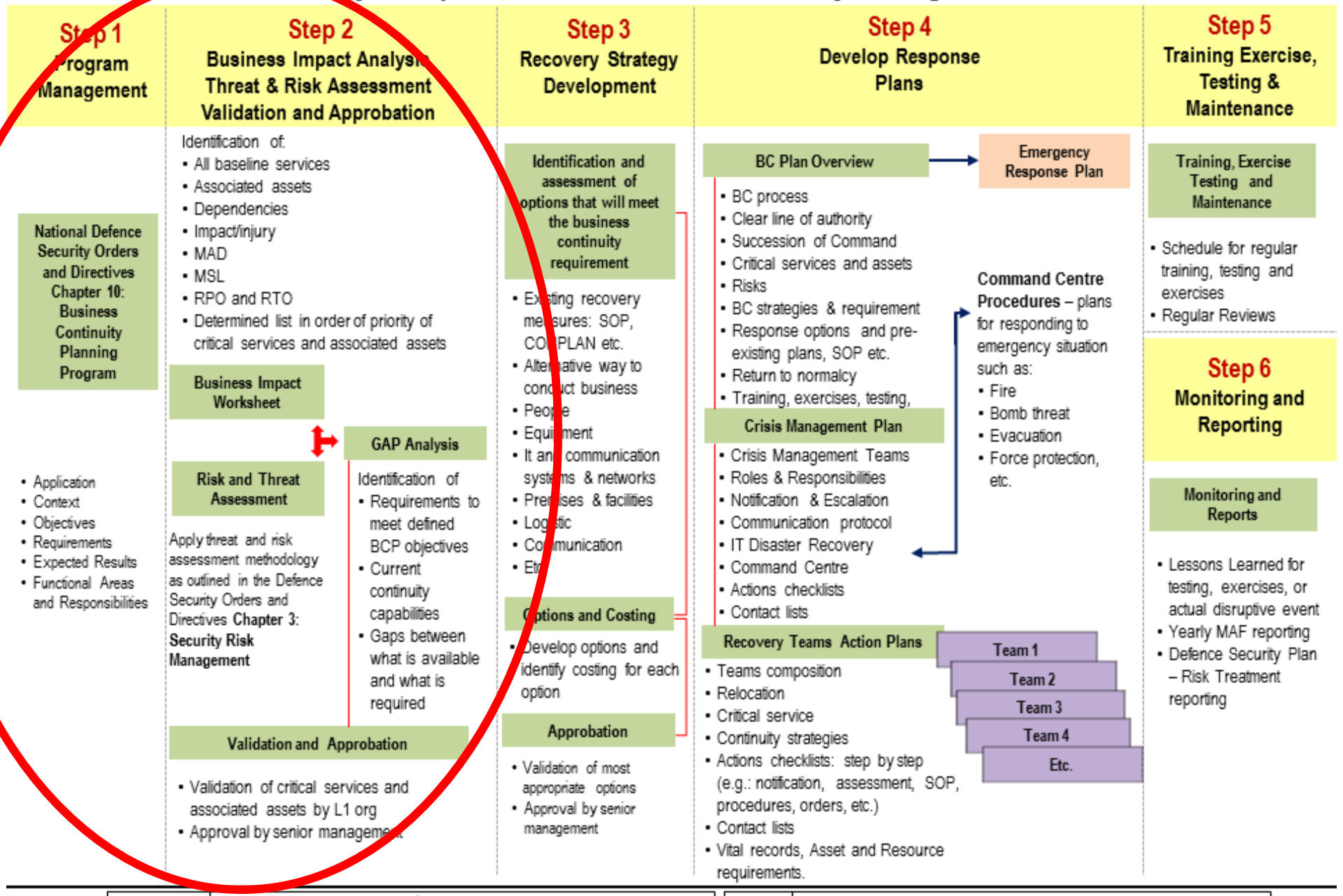
Threat and Vulnerability Assessment

Identify and analyse risks with the potential to cause injury to identified critical services and associated assets (including the effectiveness of existing controls or measures)

Business Continuity Business Impact Analysis

Identification of critical services, programs and associated assets

Key Components of Business Continuity Management



BCM Mission and Vision

DGDS will optimize DND's BCM program by instrumenting a federated BIA production in order to produce an evergreen Critical Services list that is both relevant to DND and meets TBS requirements.

Take aways

- Manage complexity - Reframing
- Main effort and supporting efforts
- Business Impact Analysis (at the strategic level) **THE KEY** first step (but hard to conduct and manage)
- Access to Leadership
- Organisational Culture

Discussion/Questions

Merci!