

Evaluation of the Duty of Care Envelope, 2017-18 to 2022-23



Evaluation Report

Prepared by the Evaluation Division

Global Affairs Canada

September 2024



Table of contents

3	Acronyms and symbols	41	Recommendations and considerations
5	Executive summary	45	Annexes
6	Program background		
10	Evaluation purpose, scope and methodology		
15	Findings: Relevance and responsiveness		
19	Findings: Effectiveness		
30	Findings: Efficiency and coherence		
39	Conclusions		

Acronyms and symbols

2SLGBTQI+	2-Spirit, lesbian, gay, bisexual, transgender, queer, intersex and additional people who identify as part of sexual and gender diverse communities	FGD	Focus group discussion
ACM	International Platform Branch	FTE	Full-time equivalent
ADM	Assistant Deputy Minister	GAC	Global Affairs Canada
BTA	Baseline threat assessment	GATE	Governance, Access, Technical security and Espionage
CBS	Canada-based staff	GBA Plus	Gender-based analysis plus
CED	Security Emergency Management, Strategy, and Policy Bureau	GoC	Government of Canada
CFM	Consular, Security and Emergency Management Branch	GSF	Global Security Framework
CIPP	Critical Infrastructure Protection Program	HCM	People and Talent Management Branch
DG	Director General	HET	Hazardous Environment Training
DND	Department of National Defence	HQ	Headquarters
DoC	Duty of care	IFM	International Security and Political Affairs Branch
DSIP	Departmental Security Investment Plan	IM/IT	Information Management/Information Technology
DSP	Departmental Security Plan	KII	Key informant interview
EGM	Europe, Arctic, Middle East and Maghreb Branch	LES	Locally engaged staff

Acronyms and symbols

MC	Memorandum to Cabinet	SCM	Corporate Planning, Finance and Information Technology Branch
MPSE	Minor physical security enhancements	SECCOM	Security Committee
MPSS	Military Police Security Services	SIMS	Security Information Management System
MRP	Mission Readiness Program	SIPAB	Security Investment Planning Advisory Board
MRT	Mission readiness team	SLP	Service line project
MSRM	Mission Security Risk Model	SMGF	Security Management and Governance Framework
OAG	Office of the Auditor General	SPA	Special purpose allotment
OGD	Other government departments and agencies	SSAMA	Strengthening Security at Missions Abroad
OPI	Office of primary interest	SSC	Shared Services Canada
PSPC	Public Services and Procurement Canada	SWD	Financial Resources Planning and Management Bureau
PSS	Personal Security Seminar	TAOMA	Threat assessment outside mission area
REMO	Regional Emergency Management Office	TB	Treasury Board
RM	Readiness Manager	USS	Office of the Deputy Minister of Foreign Affairs
RPM	Readiness Program Manager	VAR	Vulnerability assessment report

Executive summary

The evaluation of the Duty of Care (DoC) envelope, as per the 2016 DoC Memorandum to Cabinet and subsequent DoC Treasury Board submissions, covered the period from 2017-18 to 2022-23 and aimed to inform: (1) decision-making and course corrections to improve envelope delivery during the second half of its mandate; and (2) the planning of mission safety and security initiatives beyond the envelope's timeframe.

The evaluation found that the DoC envelope provided Global Affairs Canada (GAC) with unprecedented resources, increased visibility and trust as the lead security agency responsible for safety and security at Canada's missions abroad. Overall, the envelope aligned with GAC's mandate to comprehensively manage cross-mission security needs in a dynamic global security environment. Its design and initiatives were also well aligned with the department's safety and security priorities and with the needs of key stakeholders at mission. However, the evaluation found unaddressed risks across the mission network and among different stakeholder groups. A wide range of mission stakeholders identified health, safety and well being as an area that was not sufficiently addressed. Naming the envelope "Duty of Care" created confusion and led to unmet expectations even though the envelope was not intended to cover health or well-being as per the 2017 Treasury Board submission.

The envelope made progress in improving the safety and security of Canada-based staff and their dependants, locally engaged staff and visitors to Canadian missions. However, results varied among DoC-funded initiatives and across the network. One of the envelope's most important contributions was the creation of the Mission Readiness Program, which made a strong positive difference to improving mission vigilance and strengthening mission security posture. DoC-funded initiatives also contributed to strengthening the security and resilience of missions' unclassified networks and maintained the security and resilience of classified and highly classified networks. In addition, DoC investments improved decision-makers' understanding of threats and vulnerabilities and better prepared mission staff to respond to risks at mission. On the other hand, while critically important for mission security, progress on major and minor physical security projects as well as on the delivery of security equipment and systems was modest, negatively affecting the security and resilience of mission infrastructure and security posture.

The DoC envelope's structures, systems, processes and tools were designed and put in place to facilitate a comprehensive, responsive and risk-based approach to managing finite security resources. However, several challenges affected DoC delivery, including: COVID-19 and resulting operational difficulties; the complex delivery structure and the lack of a comprehensive departmental security policy that led to inefficiencies in coordination and collaboration; challenges with the envelope's prioritization of funding and programming; the limited challenge function enacted by DoC governance; and issues related to human resources, tracking and reporting and procurement. Despite these difficulties, responsible DoC stakeholders demonstrated a high level of awareness and worked to address these challenges, enabling gradual improvement to envelope delivery.

Summary of recommendations: 2017 à 2027 DoC envelope

1. Improve risk assessment models, methodologies, processes, systems and tools to assess the threats and vulnerabilities experienced across the mission network and develop well-scoped, prioritized mitigation measures.
2. Strengthen the DoC governance structure to ensure effective prioritization and allocation of resources and provide greater oversight of investments in high-risk and critical-risk missions.
3. Address remaining challenges for major and minor physical security projects, equipment and systems, and ensure timely project delivery to meet DoC envelope commitments.
4. Develop a strategy to evolve the Mission Readiness Program to ensure alignment with mission needs, existing readiness team capacity and in consideration of available resources.

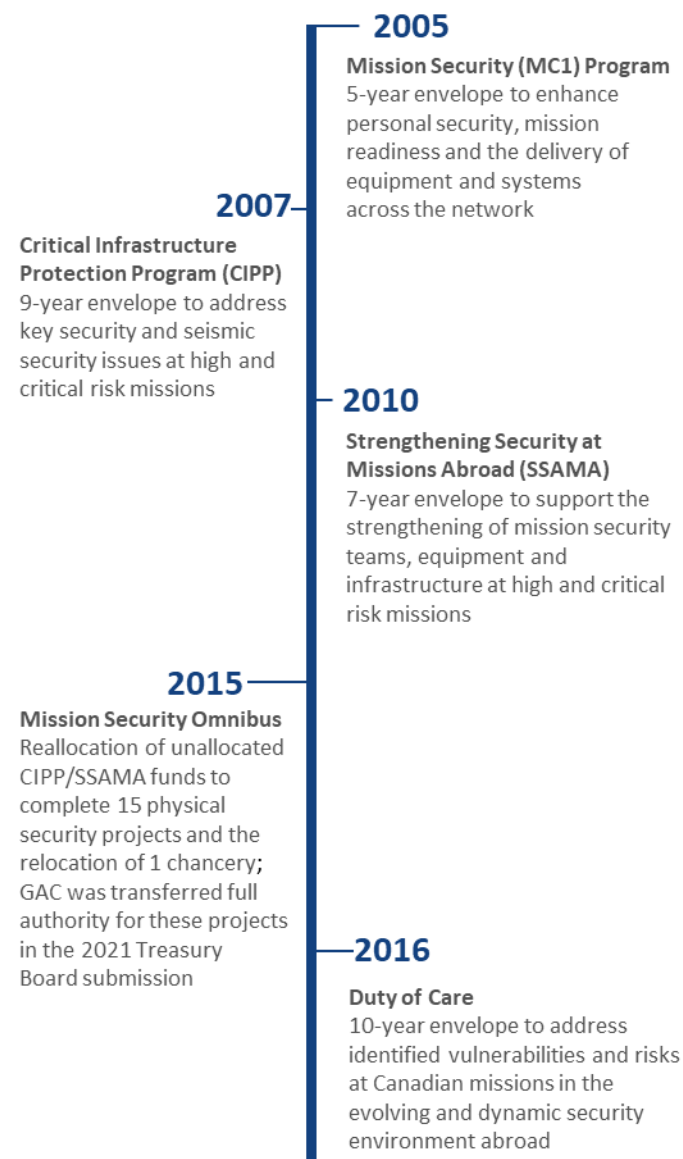
Summary of recommendations: Forward-looking (beyond 2027)

5. Develop a comprehensive departmental security policy and guidance that articulate up to date authorities, responsibilities and accountabilities for the planning and delivery of mission safety and security investments and programming.
6. Define and communicate the full scope of departmental responsibilities to protect people, information and assets at missions abroad and develop resourcing strategies to meet these responsibilities.

Program background

Background

Mission security investments timeline

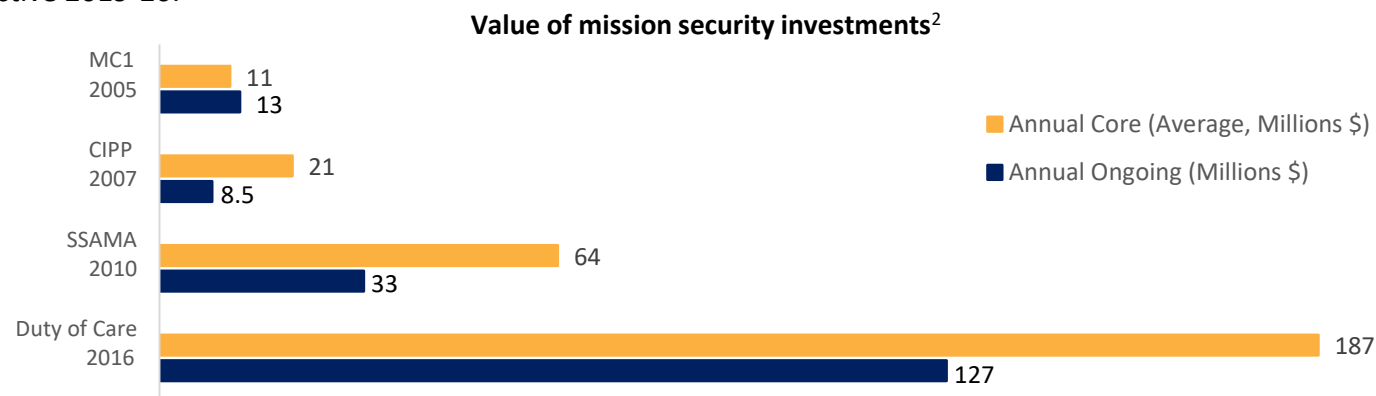


Government of Canada investments in mission security

As per the 2019 *Policy on Government Security*, Global Affairs Canada (GAC) is the lead security agency for Canada's network of missions abroad, comprised of 178 missions in 110 countries.¹ GAC is responsible for ensuring the safety and security of Canada-based staff (CBS) and their dependants, locally engaged staff (LES) while on duty, as well as visitors and invitees to Canadian missions. GAC is also responsible for Government of Canada partners and co-locators, including provinces and foreign governments hosted within Canada's missions.

In the years following the events of September 11, 2001, a number of significant investments were made to bolster security and address the broadening set of security-related issues at Canadian missions abroad: **Mission Security (MC1) Program (2005)**; **Critical Infrastructure Protection Program (CIPP; 2007)**; **Strengthening Security at Missions Abroad (SSAMA; 2010)** (CIPP and SSAMA were merged into 1 special purpose allotment [SPA] in 2010-11); and the **Mission Security Omnibus (2015)** (see sidebar and graphic below for details).

In 2016, the results of the Mission Security and Personal Safety Abroad Evaluation (see Annex I) and the sun-setting of previous security funding by 2019 prompted the department to submit a Memorandum to Cabinet (MC) entitled "**Duty of Care: Protecting Our People Through Infrastructure, Mission Readiness and Securing Our Information Abroad.**" In Budget 2017, the Department of Finance approved the allocation of **\$1.87B over 10 years (2017-18 to 2026-27) and \$127M in ongoing annual funding for the DoC envelope**. The envelope also absorbed the remaining funds from MC1 and CIPP/SSAMA; the 3 envelopes were merged as 1 fund effective 2019-20.



¹ As per the 2022-23 DoC Annual Report and 2022-23 Departmental Results Report.

² All values are represented as an average amount of funding per year (total/# of years), quoted in current \$CAD.

Background

Global Affairs Canada's legal duty of care (DoC) responsibilities in relation to the DoC envelope

Legal DoC: Under Part II of the Canada Labour Code (Part II, ss. 124 and 125) and Canadian common law, GAC must take **reasonable care** to avoid foreseeable harm to its employees (CBS and LES) as well as to CBS dependants, contractors and visitors to Canadian missions. However, what constitutes “reasonable care” is dependent on the appropriate **standard of care**, which varies across individuals and contexts. The standard of care owed to an individual is based on several determining factors, including: the nature of the relationship between the 2 parties; the type of potential harm; the specific context and circumstances; and the availability and cost of mitigation measures.

DoC envelope: While there is overlap between GAC’s legal DoC responsibilities and the 4 pillars of the DoC envelope, the two are not equivalent. The department’s responsibilities and obligations under the DoC envelope are limited only to what is articulated in the DoC Memorandum to Cabinet and subsequent TB submissions which do not necessarily cover all of GAC’s legal DoC responsibilities. For example, the 2017 TB submission intentionally did not include references to “health” or “well-being” in the envelope’s scope.

Overview of the Duty of Care envelope

The 2016 Duty of Care (DoC) MC presented a comprehensive approach to mission security and outlined a series of initiatives to mitigate the risks associated with the current and evolving security environment abroad. The purpose of this comprehensive approach was to ensure the **safety** and **security** of CBS and their dependants, LES on duty, as well as visitors and invitees to Canada’s missions through 4 pillars:

1. **Protecting Our People Through Infrastructure:** physical and seismic security enhancements and relocations/consolidations
2. **Protecting Our People Through Securing Our Information:** IM/IT support and security intelligence
3. **Protecting Our People Through Enhancing Mission Readiness:** mission security personnel, equipment and systems, training for mission staff, and contracting local security guards
4. **Protecting Our People in Kabul:** full cost of operations at the KABUL mission

In October 2017, the Treasury Board Secretariat approved GAC’s Duty of Care submission to access approximately \$1.18B in DoC envelope funding. The department also received \$105M in ongoing funding. The remaining funding was allocated to GAC through a series of additional Treasury Board (TB) submissions (see Annex II). The most recent funding was approved in December 2021 and provided GAC with more than \$430M over 6 years (\$8.4M is ongoing funding). The DoC funding envelope also absorbed an additional \$138M from CIPP/SSAMA and accompanying commitments. The DoC envelope should not be conflated with GAC’s legal DoC responsibilities which are not necessarily covered under the DoC envelope (see sidebar for details).

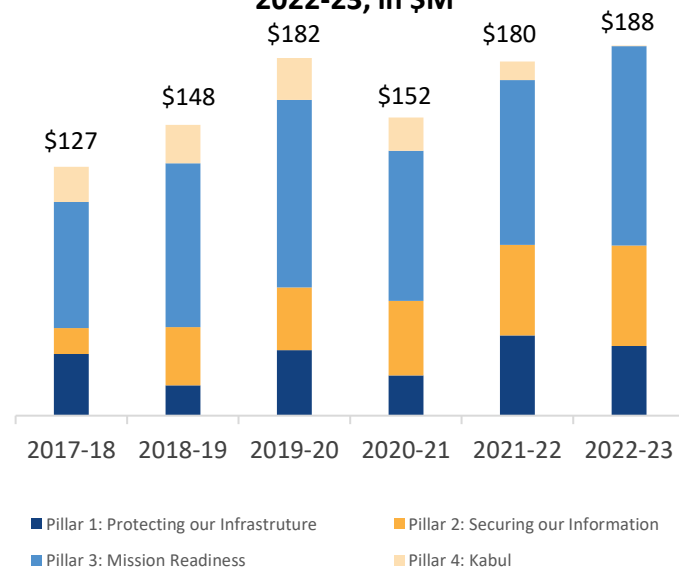
Roles, responsibilities and governance

The management and governance of the DoC funding envelope, as well as the planning and implementation of DoC-funded initiatives, were a shared responsibility among several branches of the department. The 5 main branches involved were International Platform (ACM); Consular, Security and Emergency Management (CFM); People and Talent Management (HCM); International Security and Political Affairs (IFM); and Corporate Planning, Finance, and Information Technology (SCM) (see Annex III for details). Missions and other branches (including Well-being Ombud and Inspector General [ZID]) and the geographics were also involved in implementing DoC-funded initiatives.

Three governance committees were responsible for approving and overseeing DoC funding and programming: the Security Investment Planning Advisory Board (SIPAB), Security Committee (SECCOM) and the Assistant Deputy Minister (ADM) DoC Oversight Committee (see Annex IV). CFM was responsible for tracking and reporting on progress (including annual reports to the Treasury Board Secretariat) and was the secretariat for DoC governance committees.

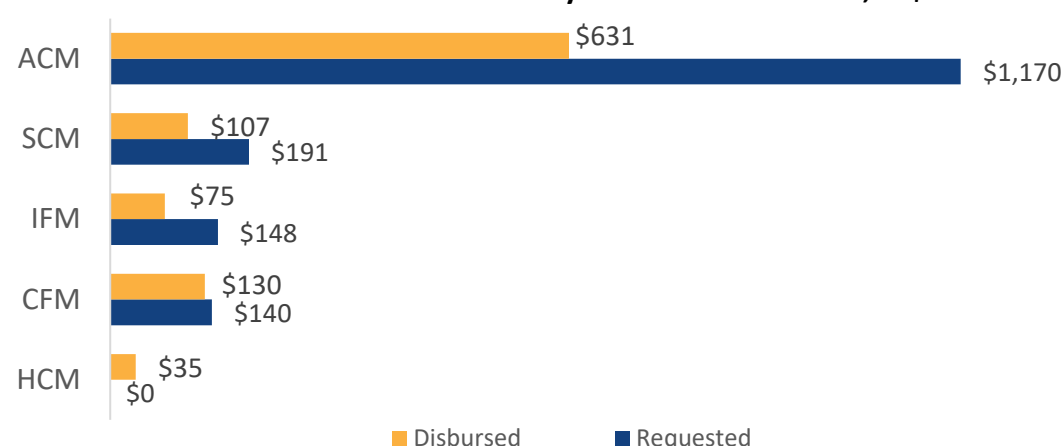
Resources

Annual DoC disbursements by pillar as of 2022-23, in \$M



The **\$1.87B DoC envelope** was distributed by branch as shown below. To date, GAC has accessed **\$1.65B** of these funds. The total disbursement from 2017-18 to 2022-23 was **\$976M**, approximately **52%** of the requested funds from 2016. The graph below shows the total disbursements by branch between 2017-18 and 2022-23 relative to the original amounts requested.

DoC disbursements by branch as of 2022-23, in \$M



Top DoC disbursements by mission, in \$M (2017-18 to 2022-23)

- | | |
|-----------------------------|----------------------------------|
| 1. Kabul
Canada \$84 | 2. Beijing
Canada \$13 |
| 3. Nairobi
Canada \$13 | 4. Port au Prince
Canada \$11 |
| 5. London
Canada \$9.3 | 6. Mexico City
Canada \$8.6 |
| 7. Kingston
Canada \$7.6 | 8. Dakar
Canada \$6.4 |
| 9. Manila
Canada \$5.7 | 10. Islamabad
Canada \$5.7 |

Annual disbursements (see sidebar) saw an initial expenditure of \$127M in 2017-18, with subsequent years averaging just over \$170M per year. The COVID-19 pandemic and resulting operational difficulties led to a noticeable decline in expenditures in 2020-21. However, the envelope has rebounded since, with its highest expenditure to date taking place in 2022-23; this was despite the suspension of mission operations in KABUL in August 2021, which significantly reduced expenditures under Pillar 4.

From 2017-18 to 2022-23, the envelope focused a significant proportion of resources (\$504M, or 52% of the envelope disbursements) on mission readiness (Pillar 3). Pillar 3 encompassed all DoC-funded initiatives focused on mission preparedness and enhancing mission vigilance and security posture. These investments were managed by both ACM and CFM and included the preparation and deployment of Mission Readiness Program personnel and local security guards, the procurement and delivery of security equipment and systems, and the provision of security-focused training.

As of March 2022, there were also 135 pressure/reallocation requests (106 were approved, for a total of \$325M in disbursements).

Evaluation purpose, scope and methodology

Evaluation purpose, scope and objectives

Evaluation scope

The evaluation scope focused on the initiatives and projects funded between 2017-18 to 2021-22 under the 2016 MC *“Duty of Care: Protecting Our People Through Infrastructure, Mission Readiness and Securing Our Information Abroad”* and related TB submissions. However, given the evaluation timeline, information and data pertaining to DoC implementation beyond 2022 was included where possible. **This evaluation scope did not include the department’s legal DoC responsibilities that were not covered under the DoC envelope.**

The evaluation encompassed all 4 DoC envelope pillars. In addition, the evaluation scope included GAC systems, structures and processes related to the planning, management and governance of the DoC envelope. The evaluation also considered the broader context in which the envelope was designed and implemented, including global security trends, like-minded actors in the security environment, and the COVID-19 pandemic. The evaluation did not include other GAC security-related programs, projects and activities that were not funded by the DoC envelope, even when they were implemented by the same branches involved in delivering DoC-funded initiatives.

³Key stakeholders: DoC decision-makers, implementers and beneficiaries (Canada-based staff, their dependants, locally engaged staff while on duty and visitors/invitees to missions).

The evaluation was conducted in line with the 2016 DoC MC and all subsequent DoC TB submissions, the Five-Year Departmental Evaluation Plan and the Treasury Board *Policy on Results*. The intended primary evaluation users included the DoC envelope’s offices of primary interest (ACM, CFM, HCM, IFM, SCM), as well as management and staff involved in DoC planning and delivery at both HQ and missions.

Evaluation purpose and objectives

The evaluation’s purpose was to 1) generate insights, findings, conclusions and recommendations to inform decision-making, course corrections, and improvements on how best to deliver the DoC envelope effectively and efficiently during the second half of its mandate; and 2) provide evidence and lessons learned to inform future planning for safety and security initiatives beyond the 2016 MC timeframe (2017-18 to 2026-27).

The objectives of the evaluation were to assess:

- the relevance and responsiveness of the DoC envelope to the priorities of the department and the Government of Canada, and to the needs and priorities of key stakeholders³
- the progress to date of the DoC envelope
- the extent to which systems, structures and processes have enabled and/or hindered the effective, efficient and coherent implementation of the DoC envelope

Evaluation approach

The evaluation was grounded in several complementary approaches to meet its purpose and objectives:

- **Formative evaluation:** Given that the evaluation took place during the midpoint of the envelope’s implementation timeframe, a formative evaluation approach was applied to inform improvements and course corrections to its delivery while activities were still in progress.
- **Utilization-focused evaluation:** The evaluation was intentionally and explicitly designed and implemented to meet the information needs of the intended evaluation users.
- **Mixed methods with a GBA Plus lens:** The evaluation employed a mixed-methods approach, gathering data from a diversity of sources and drawing on both qualitative and quantitative data. The evaluation team used different types of triangulation techniques to ensure the validity and reliability of findings, conclusions and recommendations. The evaluation also applied a gender-based analysis plus (GBA Plus) lens to assess how diverse groups of people experienced DoC-funded initiatives and their results at mission.
- **Case study approach:** The evaluation conducted 8 case studies to provide a rich, in-depth understanding of the main evaluation issues across a selection of Canadian missions and their operational contexts.

Evaluation questions

The evaluation team assessed 4 main issues: 1) relevance and responsiveness, 2) effectiveness (results), 3) efficiency and 4) coherence. For each issue, evaluation questions and sub-questions were developed through a participatory design process, involving representatives from the various branches involved in DoC planning and delivery. From these key questions, an evaluation matrix was developed to serve as the guiding framework for the evaluation. Below is a simplified version of the matrix, which details the evaluation issues, evaluation questions and sub-issues. Key findings corresponding to each sub-issue are also identified (see Annex V for a detailed version).

Evaluation issue ⁴	Key evaluation questions	Sub-issues (corresponding findings)
Relevance and responsiveness	1. To what extent was the DoC envelope relevant and responsive to the needs and priorities of key stakeholders?	1.1 DoC envelope's alignment with GAC's mandate, policies and priorities (<i>Findings 1 and 2</i>) 1.2 DoC envelope and funded initiatives' alignment with safety and security needs of stakeholders (<i>Findings 2 and 3</i>) 1.3 DoC envelope and funded initiatives' responsiveness to the evolving needs of stakeholders (<i>Findings 1, 4 to 9, 13, 15, 16, 18, and 19</i>) 1.4 DoC-funded initiatives' alignment with the original parameters of the 2017 DoC TB submission (<i>Findings 2 and 3</i>)
Effectiveness (results)	2. What progress has the DoC envelope made to achieving its objectives and results to date?	2.1 Results obtained through DoC envelope funding (<i>Findings 4 to 12</i>) 2.2 Experience of DoC envelope results by different stakeholder groups (<i>Finding 11</i>) 2.3 DoC envelope progress toward its intended purpose as per the 2017 TB submission (<i>covered under 2.1</i>) 2.4 Factors that affected progress toward results (<i>Findings 4 to 20</i>)
Efficiency	3. To what extent did the DoC envelope structures, systems and processes ⁵ enable and/or hinder it to deliver on its mandate?	3.1 DoC envelope structures, systems and processes that enabled and/or hindered its delivery (<i>Findings 13 to 20</i>) 3.2 DoC envelope structures, systems and processes that enabled and/or hindered the timely allocation of funding to address needs (<i>covered under 3.1</i>) 3.3 DoC envelope structures, systems and processes that enabled and/or hindered an accurate prioritization of funding and programming (<i>Findings 15 and 16</i>) 3.4 DoC envelope structures, systems and processes that enabled and/or hindered its ability to define, track, measure, and report on results (<i>Finding 17</i>)
Coherence	4. To what extent was the DoC envelope implemented in a coherent manner?	4.1 Coordination and cooperation between the departmental units responsible for operationalizing the DoC envelope (<i>Findings 14, 15, 19 and 20</i>) 4.2 Understanding of DoC envelope definition and purpose (<i>Findings 1 to 3</i>)

⁴ COVID-19 was considered as a cross-cutting theme for all evaluation questions.

⁵ Examples of structures, systems and processes included but were not limited: DoC governance structures and processes, DoC business processes, IM/IT systems and processes, organizational structures and division of responsibilities.


Evaluation methodology

The following lines of evidence were used for the evaluation. For more details, see Annex VI.

Document review	Financial analysis	Environmental scan of DoC policies and approaches used by Canada's allies
<p>The evaluation included a review of internal and external documents including but not limited to:</p> <ul style="list-style-type: none"> • GAC security-related frameworks, governance and planning documents • Annual TB reports/other DoC envelope reporting products • Departmental Security Plan (DSP) implementation matrix and other tracking tools • Security programming literature 	<p>The evaluation collected financial information for the period 2017-18 to 2022-23, which spanned all DoC-funded initiatives and projects.</p> <p>The financial analysis of DoC envelope expenditures was completed to better understand the allocation and use of government resources to deliver the initiatives funded through the envelope.</p>	<p>An environmental scan of how Canada's security partners operationalized their duty of care responsibilities was conducted to identify key information, best practices and lessons learned related to like-minded countries' DoC-related policies, approaches and programs. The study included a literature review and interviews with officials from Australia, Germany, Italy, the Netherlands, Spain, the United Kingdom, the United States and the European Union as well as 6 detailed comparative country cases (United States, Australia, France, Germany, United Kingdom and European Union).</p>
Online survey	HQ key informant interviews (KIIs)	Mission case studies
<p>The evaluation included an online survey with DoC decision-makers/implementers and DoC beneficiaries (mission staff, both CBS and LES, as well as CBS dependants).</p> <p>Survey questionnaires incorporated a GBA Plus lens to ensure representation within and among stakeholder groups.</p> <p>The survey was sent to 157 heads of mission (HOM), 121 heads of security, 919 CBS (including other government departments) and 895 LES. It achieved an overall response rate of 43% (891 total respondents) with representative samples for both the CBS and LES groups.</p>	<p>The evaluation team conducted 42 semi-structured KIIs, both remotely and face-to-face, with staff and management at HQ across all 5 branches involved with the DoC envelope.</p>	<p>All 8 mission case studies (1 remote and 7 field-based) employed multiple data collection methods with a variety of stakeholder groups. Methods for both remote/field mission case studies included an in-depth document review of mission specific documents and data as well as KIIs (either remotely or in person) with DoC decision-makers/implementers and, in some cases, DoC beneficiaries. Field mission case studies also included in-person focus group discussions (FGDs) and/or KIIs with DoC beneficiaries (mission staff, both CBS/LES as well as CBS dependants), and direct observation. In total, 64 KIIs and 23 FGDs (5-10 participants each) were conducted.</p> <p><i>Note: the selection of case study missions is classified.</i></p>

Evaluation limitations and mitigation measures

Limitations




Confidential/protected data: The DoC envelope evaluation required accessing, collecting, analyzing and interpreting protected and classified (i.e. secret) data, both from primary and secondary sources. This required additional protocols when analyzing and collating unclassified, protected and classified information together (e.g. for data triangulation). This also limited the information that was reported on in unclassified versions of evaluation products.

Complexity of DoC programming, dynamic operating contexts and number of key stakeholders: GAC manages a network of 178 diplomatic missions in 110 countries. Given the varied and dynamic contexts and security environments in which GAC operates, there was significant complexity and variation in the ways in which the DoC envelope was applied and experienced. In addition, the very unstable security situation at several missions affected the evaluation team's ability to conduct in-person visits or access key informants. Finally, DoC beneficiaries spanned a very wide group of people world-wide, including all staff and CBS dependants. It was therefore a challenge to directly access representative samples of these groups.

Impacts of COVID-19: Within the temporal scope of the evaluation, the COVID-19 pandemic had an anomalous impact on the way the DoC envelope was operationalized, affecting its performance in non-typical ways, including the unprecedented evacuation of many mission staff across the network.

Multiple OPIs: There were 5 offices of primary interest (OPIs) for the evaluation (ACM, CFM, HCM, IFM, SCM). With multiple decision-makers, this increased the complexity for the evaluation team to achieve agreement and validation on the evaluation findings, conclusions and recommendations.

Mitigation measures



Confidential/protected data: The evaluation team had access to the department's secure network and ensured that departmental protocols were followed when accessing, collecting, analyzing and interpreting protected and classified information. All information that was included in unclassified evaluation products was reviewed to ensure that classified information was not reported. The evaluation team made efforts to produce unclassified evaluation products, including this report, to ensure accessibility of the information without compromising sensitive and classified information. All products with sensitive and classified information are stored on appropriate platforms.

Complexity: To ensure that the evaluation captured the diverse application and experiences of DoC-funded initiatives, the evaluation team used a mixed methods approach to collect and analyze both qualitative and quantitative data from a variety of sources and methods. In addition, qualitative methods were used to cover as many operating contexts as resources allowed and to ensure that HQ staff were represented across DoC responsibility centres. For in-person case studies, efforts were made to maximize the diversity of stakeholders consulted. The evaluation also relied on a mix of in-person and remote data collection strategies. Where in-person data collection was not feasible, the evaluation team employed remote methods using available technology (e.g. for the KABUL case study). Finally, the evaluation conducted an online survey that was administered to representative samples of 4 key stakeholder groups (HOMs, heads of security, Canada-based staff and locally engaged staff).

Impacts of COVID-19: To address COVID-19 and its impact on the DoC envelope, the evaluation team incorporated it as a cross-cutting theme throughout the evaluation. It was considered in all phases of the methodology.

Multiple OPIs: The evaluation team leveraged the DoC ADM Oversight Committee as a reference group for the evaluation. In addition, each ADM identified a focal point representing its respective branch. The focal points and ADMs were engaged to elicit feedback, insights and advice at key stages throughout the evaluation and on select evaluation deliverables.

Findings: Relevance and responsiveness

Relevance and responsiveness

Evolving approaches to mission security

There is a consensus in the literature that diplomats are increasingly living with growing risks. To better adapt to the dynamic international security context, Canada's allies have significantly broadened their approach to diplomatic security. While earlier approaches to protection were largely based on traditional notions of hard security for people, infrastructure and information, today's approaches are increasingly focused on the safety and well-being of personnel abroad, and include diplomats' dependants as well as LES (Environmental Scan, 2023).

Finding 1: The Duty of Care envelope built on the department's evolving approach to mission security and aligned with GAC's mandate to comprehensively manage cross-mission security needs in a dynamic global security environment.

Global Affairs Canada manages a network of 178 missions, made up of over 8000 Canada-based staff (CBS) and locally engaged staff (LES) in 110 countries. To effectively fulfill its mandate to advance Canada's international relations, and associated responsibilities with regards to foreign policy, trade and international assistance initiatives and to provide consular services to Canadians, the department requires a significant presence on the ground. As a result, **Canada's diplomatic missions operate within a wide spectrum of dynamic and evolving security contexts.** Effective representation in these contexts depends on a sophisticated understanding of threats and vulnerabilities across the network, as well as the effective and responsive mitigation of context-specific security risks at a given mission location.

The DoC envelope represented the Government of Canada's largest investment in mission security to date, amounting to more than double the total investments from the 3 previous special purpose allotment (SPAs) combined. The envelope's scope and magnitude brought about **increased visibility** for mission security within the department and **reinforced trust and confidence in GAC** to provide leadership, advice and guidance to protect Canadian diplomatic missions abroad (as mandated in the 2019 *Policy on Government Security*). The Treasury Board's approval of the DoC funding envelope in 2017 also bolstered the department's evolving and more comprehensive approach to mission security and solidified its transition-from the conventional "gates, guns and guards" model of the earlier Critical Infrastructure Protection Program and Strengthening Security at Missions Abroad (CIPP/SSAMA) SPA, which focused heavily on physical infrastructure. The DoC envelope placed an **additional emphasis on protecting people, through securing information and enhancing mission readiness** in response to the dynamic nature of security risks across the mission network. This approach explicitly included the safety and security of CBS, their dependants, LES (while on duty), and visitors to Canadian missions. GAC's evolving approach to mission security was also fully in line with observed trends among Canada's allies and like-minded security partners (see sidebar).

The DoC envelope was designed in accordance with the *Policy on Government Security* to comprehensively address cross-mission safety and security needs and respond to evolving global security threats, which have increased in complexity, sophistication and geographic reach in recent years. More specifically, the envelope's design was grounded in **3 foundational concepts** that are essential for successful security programming: **risk-based prioritization, evidence-based decision-making** and the **capacity to respond to emerging risks.** To this end, specific structures, processes and mechanisms were built into the envelope's design to align with these foundational concepts (see Finding 13).

Relevance and responsiveness

Table 1: Departmental Security Plan priorities

2019-20 Departmental Security Plan priorities	
1.	Strengthen mission infrastructure abroad
2.	Enhance mission readiness
3.	Mitigate cyber and information security risks
4.	Strengthen business continuity planning and emergency management
5.	Reinforce security culture and awareness

Source: 2019-20 Departmental Security Plan

Table 2: Top departmental strategic risks

Mission Network Risk Profile (2023-24)	Enterprise Risk Profile (2022-24)
1. HR and workforce capacity	1. Health, safety, and well-being (resilience and retention)
2. Management of security and crises	2. Health, safety, and well-being (health at missions)
3. External forces	3. Cyber/digital security and resilience
4. Health, safety and well-being	4. IT infrastructure
5. External engagement	5. Management and security of real property and assets

Sources: 2023-24 Mission Network Risk Profile and 2022-24 Enterprise Risk Profiles

Finding 2: The DoC envelope and initiatives broadly aligned with the department's security priorities, and mostly addressed the safety and security needs identified by mission stakeholders.

While the department did not have a concrete security policy (see Finding 14), several departmental frameworks highlighted GAC's safety and security-focused priorities. For example, security at mission was an integral element in 2 out of the 5 core responsibilities in the departmental results framework (DRF) (Core Responsibility 4 - Help for Canadians Abroad, and Core Responsibility 5 - Support for Canada's Presence Abroad). In addition, GAC's Enterprise Risk Profile (ERP) (previously "corporate risk profile") provided an overview of the top strategic risks that affected the department, including those across the mission network. Additionally, the Mission Network Risk Profile (MNRP) highlighted the wide range of risks unique to missions abroad.

The safety and security priorities listed within these frameworks were linked directly to the Departmental Security Plan (DSP)⁶. Since 2019, the DSP has identified 5 security priorities (see Table 1), which if not mitigated, could compromise the department's ability to safeguard its people, information and assets abroad. Based on an assessment of the DoC envelope's original design as per the 2017 TB submission and the full spectrum of initiatives funded through the envelope, **evaluation evidence clearly highlighted that the envelope fully aligned with the security priorities outlined in the DSP**. In addition, there was strong alignment between the envelope and the ERP and MNRP, in particular in the areas of cybersecurity, IT infrastructure, security of real property, and management of security and crisis events (see Table 2). However, a gap between the DoC envelope/DSP priorities and those in the ERP and MNRP was noted in the area of health, safety and well-being (see Finding 3).

Moreover, **the envelope's design** (e.g. threat and vulnerability categories), as well as the corresponding initiatives funded through DoC TB submissions, **aligned with the primary safety and security concerns identified by survey and case study respondents, with some exceptions** (Finding 3). Evidence demonstrated that the most pressing cross-mission risk overall was to personal safety (criminality), followed by espionage, natural disasters, civil unrest, terrorism and armed conflict. Interestingly, both male and female survey respondents identified the same top three threats at nearly identical frequencies. For a detailed analysis of differential risks across the diverse stakeholder groups at mission, see Findings 3 and 11.

⁶The DSP includes, but is not limited to, the investments under the DoC envelope as it covers all departmental security, including domestic security.

Relevance and responsiveness

Health, safety and well-being and the DoC envelope

While Global Affairs Canada owes a legal “duty of care” to its employees, CBS dependants, contractors and visitors to Canadian missions abroad, these responsibilities were not necessarily covered under the DoC envelope’s scope (see p.11 for details). While “health and security mission incidents” were later added to the envelope’s scope in 2018-19, the additional funding was not sufficient to meet stakeholder needs.

The analysis supporting Finding 3 is therefore related to the relevance of the envelope in relation to identified stakeholder safety and security priorities and is not a judgment on the effectiveness of the envelope relative to its stated objectives (the latter is covered by Findings 4 to 12).

Finding 3: Despite the envelope’s broad alignment to needs, there were additional safety and security priorities identified directly by key stakeholders and within departmental risk frameworks that were not part of the original DoC envelope design, notably in the area of health, safety and well-being.

Despite the envelope’s broad alignment with departmental priorities and key stakeholders' safety and security needs (Finding 2), **evidence highlighted other priority departmental risks as well as additional safety and security concerns identified by mission stakeholders that were not included in the original DoC envelope design.** One key area was health, safety and well-being. Case study and survey evidence highlighted this as a priority risk for mission staff and CBS dependants, who felt underserved by available departmental resources (including, but not limited to, the DoC envelope). Specifically, there was a **lack of departmental coverage in areas critical to the successful pre-deployment preparation, deployment and post-deployment reintegration of mission staff.** Psychological, health and fitness assessments, as well as stress management and conflict resolution training, were identified as pre-deployment gaps. Moreover, the additional support envisaged for deployment in conflict zones, such as rest and relaxation travel and Employee Assistance Program (EAP) visits, was scaled down due to COVID-19. That said, the 2021 DoC TB submission included funding for expanding EAP in higher-risk missions on a pilot basis.

Health, safety and well-being was also identified as a top risk within departmental risk frameworks, including the Enterprise Risk Profile and the Mission Network Risk Profile (see Finding 2, Table 2). For Canada’s security partners, initiatives focused on health, safety and well-being were increasingly included in their government’s DoC policies (e.g. United States, United Kingdom, the Netherlands). By **naming the envelope “Duty of Care,” there was persistent confusion among DoC responsibility centres on whether health, safety and well-being should be considered in the DoC envelope’s scope,** given the broader legal DoC implications and the fact that other GAC and Health Canada programming covered elements related to health, safety and well-being at mission (see sidebar and Finding 20).

Mission stakeholders also reported additional risks that were not adequately addressed through DoC envelope resources. For example, LES faced harassment from their clients (both during and outside of work hours) and reported a lack of tools and training to support them. Often being unfamiliar with local traffic laws and customs, CBS expressed road safety as a major concern for which appropriate training was infrequently provided. Compliance and complacency (e.g. handling of documents, building access procedures, respecting movement protocols) among CBS staff and their dependants were noted by decision-makers as important risks that required increased attention from DoC envelope resources. Finally, racism and discrimination were identified by affected groups at mission as risks that were not sufficiently accounted for in the scope of DoC initiatives (for additional GBA Plus on risks, see Finding 11).

Findings: Effectiveness

Note: The evaluation team developed and validated a DoC envelope theory of change (see Annex VII) as a tool to frame and measure the envelope's progress toward achieving its objectives and results. The theory of change was informed by existing performance measurement frameworks related to DoC tracking and reporting.

While there are distinct result chains under each pillar at the activities and output levels, expected outcomes are interlinked and interconnected across all DoC pillars and initiatives. Therefore, the findings on effectiveness are presented under each expected outcome rather than by pillar. While the KABUL case study evidence contributed to the main findings in the report, specific lessons from DoC programming in KABUL are detailed in Annex VIII.

Effectiveness

Security and resilience of mission infrastructure

Pillar 1 Physical security investments

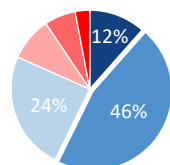
\$480M was allocated for 26 **major capital projects (MCPs)**: 13 physical security enhancements, 9 relocations/consolidations and 4 seismic enhancements. In addition, 23 legacy CIPP/SSAMA projects were included under the DoC scope.

\$36M (over 10 years) was allocated for **minor physical security enhancements (minor projects)** to address small physical upgrades and vulnerabilities up to \$500K. In 2023, MPSE was rolled into a new category called service line projects with security equipment and systems.

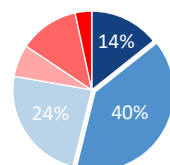
Mission survey results



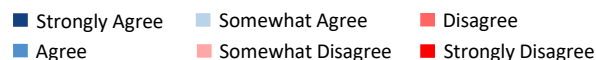
Physical security upgrades were identified as the **3rd MOST EFFECTIVE** DoC initiative at addressing mission security needs.



82% of DoC decision-makers at least **somewhat AGREED** that safety and security initiatives had contributed to reducing physical vulnerabilities at their mission (3rd highest ranked out of 5 DoC expected results).



78% of DoC beneficiaries at least **somewhat AGREED** that safety and security initiatives had strengthened their mission's physical infrastructure (lowest ranked out of 5 DoC expected results).



Finding 4: DoC investments in strengthening mission physical infrastructure were critical for improving the safety and security of people across the network. However, slow project delivery, due to both internal and external challenges, limited the department's ability to address physical vulnerabilities at missions. Recent efforts have been made to address inefficiencies and boost capacity to improve project delivery.

Evidence highlighted that **Pillar 1 physical security enhancement initiatives** (major and minor projects, see sidebar), **when delivered in a timely fashion, made a positive difference** to strengthening the security and resilience of missions' physical infrastructure. Physical security upgrades were ranked as the third most effective DoC initiative by decision-makers at mission, though DoC beneficiaries were less positive about their contribution to strengthening mission infrastructure (see sidebar). However, evidence from the document review, interviews, case studies and mission survey demonstrated that **progress towards delivering both major and minor projects was slow and encountered multiple delays (see next page)**. According to the survey, more than 1 out of 3 DoC decision-makers (37%) reported that the required physical security enhancements for their mission had not been completed or were not progressing according to schedule. This was the lowest score among 8 widely delivered DoC initiatives (see Annex IX for ranked survey results for DoC initiatives and results).

Since 2017, at the midway point in the DoC envelope, construction on a total of 9 major capital projects was completed. According to the 2022-23 DoC annual report and the 2023-24 ACM mid-year progress report, this included **1 of the original 26 projects** identified in the 2017 TB submission (Buenos Aires); **the interim Moscow co-location project** (the original Moscow relocation project is permanently on hold); and **7 out of the 23 legacy Critical Infrastructure Protection Program (CIPP)/ Strengthening Security at Missions Abroad (SSAMA) (CIPP/SSAMA) projects**. Physical security concept design objectives were also met on another 3 CIPP/SSAMA projects. Across case studies, respondents at missions with planned major projects expressed frustration with long project timelines. A common sentiment among missions with a scheduled relocation project was that physical security investments for their current chancery were not prioritized or even canceled. Faced with delays, respondents felt that important physical security vulnerabilities at their current chancery were not being addressed, compromising their safety while they waited for their relocation project to be completed.

Given the **discrepancies and inconsistencies in reporting, progress on minor projects was difficult to assess** (see Finding 17). According to the 2022-23 annual report, there were a total of 435 minor projects since 2017. Of those, 194 minor projects were "completed or closed"; however, it was not clear how many were completed versus closed for other reasons. Another 241 projects were in implementation. In the 2021-22 annual report, the total number of minor projects planned and delivered since 2017 was questionably higher (523 projects), with a reported 10% (54 projects) completed and nearly half (255 projects) still at the planning stage.

The planning and delivery of both major and minor projects were hindered by multiple internal and external challenges as detailed on the next page.

Effectiveness

Security and resilience of mission infrastructure

ACM's responses to identified challenges

ACM challenge	ACM response
Cumbersome internal governance processes	The Investment and Project Management Framework (IPMF) was put in place in 2020 to improve governance (multi-tiered approvals and committees) and streamline processes related to major projects. The Service Line Project Management Framework (SLPMF) also simplified the governance for minor projects, equipment and systems (now service line projects [SLPs]).
Structural challenges between planning and delivery functions	ACM underwent a branch-wide restructuring in 2023. As a result, feasibility assessments for major projects have progressed; minor project management is no longer split between 2 bureaus and has moved to a dedicated team.
Issues with minor project reporting	ACM established the service delivery portal (SDP) to improve tracking and reporting on SLPs.
Misalignment between the security-based prioritization and project implementation plan	CFM and ACM made efforts to improve their collaboration. Quarterly meetings have been set up to review and confirm physical security mitigation priorities. A list of top 20 priority missions has been developed.

Finding 4 (cont'd).

One of the most impactful external factors was the **COVID-19 pandemic** and resulting operational difficulties (e.g. travel restrictions) and economic impacts (e.g. inflation, supply chain challenges). Internally, the International Platform Branch (ACM) relied on overly cumbersome **governance processes**; all physical infrastructure projects over \$500K required ADM approval through the Platform Project Oversight Committee (PPOC). Minor projects were also managed under the same structure used for major projects, resulting in disproportionate oversight relative to project size. In addition, evidence pointed to **structural challenges** between the ACM's planning and delivery bureaus. For minor projects, the additional bureaucracy as well as the lack of clear roles and responsibilities between the 2 bureaus resulted in inefficiencies. For major projects, this led to challenges in the scoping/feasibility phase and delayed project delivery.

While long project timelines were expected for **major projects**, additional unique challenges further delayed their implementation. **Changes made to a major project's scope after design approval**, combined with **rising inflation, supply chain pressures and increased costs, forced ACM to re-scope or scale down some major projects** - causing further delays or even full cancellations. In addition, ACM had to manage project delivery in **dynamic, unpredictable and evolving security and political environments across the mission network**, which hindered the efficient delivery of some major projects due to the volatile contexts on the ground.

Internal issues further exacerbated delivery challenges for **minor projects**. **The demand for and complexity of minor projects were not well anticipated in the envelope's design**. Funds for minor projects were capped at \$3M per year, which was not sufficient to meet mission demand. In addition, the human resources allocated for minor projects at the onset were not adequate to keep pace with addressing missions' physical security needs. Another factor that hindered minor project delivery was the **misalignment between the prioritized list of mitigation measures provided by CFM through the countermeasure tracker on the Security Information Management System (SIMS) and the project sequencing process and implementation plan managed by ACM** (see Finding 15). Once ACM received the proposed list of countermeasures in SIMS, it took considerable time and effort to accurately define, scope and cost out the corresponding projects, further delaying implementation timelines. Finally, the delivery of minor projects was negatively affected by delays due to challenges with supply chain/procurement processes (see Findings 9 and 19 for details).

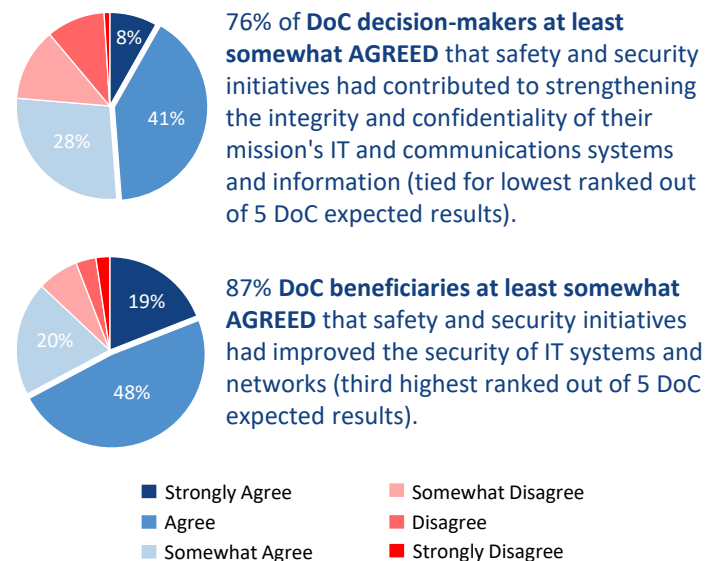
In response to these challenges, **ACM made efforts to address inefficiencies and improve their capacity to manage their portfolio** (see sidebar). However, it is too early to fully assess the impacts on project delivery.

Effectiveness

Security and resilience of the mission IM/IT network/platform

Pillar 2 of the DoC envelope focused on protecting people through securing information, with targeted investments that focused on strengthening the security and resilience of the IM/IT networks at missions abroad. IM/IT investments included funding for 4 main areas of work: mission connectivity, secret systems, information security, and network security and resilience.

Mission survey results



Finding 5: DoC-funded initiatives helped strengthen the security and resilience of the missions' unclassified network and maintained the security and resilience of classified and highly classified networks.

The visibility of IM/IT initiatives (for details on IM/IT investments, see sidebar) and their resulting improvements was limited for the average user at mission as this work generally took place behind user interfaces. Nevertheless, evidence from interviews, program reports and the mission survey (see sidebar for survey results) highlighted that the **security and resilience of the unclassified IT network/platform across the mission network were strengthened through DoC-funded improvements to connectivity and network security and the development of an IT security risk management framework in 2019**. One key development was the re-establishment of the Security Operations Centre (SOC) in 2020. The SOC produced cyber-threat intelligence analysis and reporting, monitored and analyzed cyber threats, responded to cyber incidents, and operated and maintained IT systems for the unclassified network. As it matured, it provided increasing benefits, such as faster response times to phishing incidents.

DoC investments were also critical to maintaining classified and highly classified elements of the IM/IT platform. These included the C5 upgrade project, the replacement of Secret-classified end-user devices, and the upgrading of cryptographic devices across the mission network. However, the development of new classified capabilities and communications, including GCSI Global, the C6 Fly Away Kit and mobile solutions was delayed due to difficulties in working with the infrastructure provider, Shared Services Canada (SSC), on international requirements, work-from-home protocols related to COVID-19, and resourcing challenges (see Finding 18). The expansion of highly classified platform elements throughout the mission network was also limited by its dependence on the progress of physical infrastructure projects, namely upgrades to high secure zones which had lengthy delivery timelines and were often delayed (see Finding 4).

Effectiveness

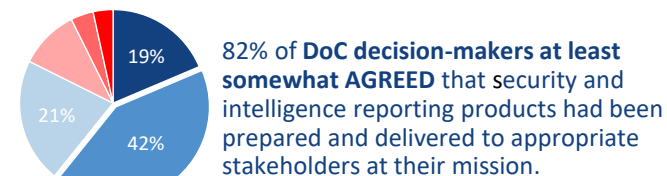
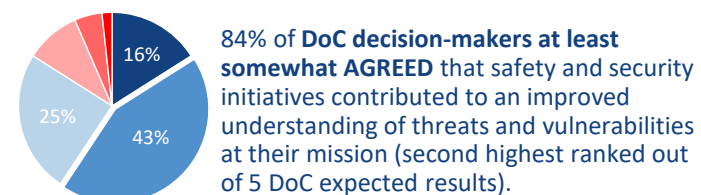
Understanding threats and vulnerabilities

Pillar 2 of the DoC envelope funded security intelligence initiatives that aimed to address GAC's need to access, collect and analyze threat-related intelligence across the mission network.

2022-23 Security intelligence outputs



Mission survey results



Finding 6: DoC investments improved decision-makers' understanding of threats and vulnerabilities at mission through increased availability and diversity of security and intelligence information and new threat analysis capacities.

Evidence from the survey (see sidebar), interviews and document review highlighted that DoC investments under Pillar 2 **increased the availability and quality of security and intelligence information for the department's decision-makers in multiple ways**. DoC contributed to increasing the **amount and diversity of security and intelligence data**. For example, GAC acquired access to new specialized datasets and security intelligence subscriptions and developed geomatic (mapping) capabilities on both SIGNET-D and more sensitive systems. In 2021, GAC launched a geomatics platform which enhanced its ability to understand, prepare for and address risks abroad.

The number of security and intelligence reporting products produced internally (see sidebar) has increased, and their quality has improved. To support decision-making, the department produced baseline threat assessments (BTAs) which provided an overview of threats in the mission area. While there were initial challenges with the timeliness and relevance of BTAs, they have evolved since 2017 and now include a GBA Plus component and an improved espionage threat analysis. Given that BTAs were not intended for operational use, threat analysts also produced operational threat assessments that were uniquely tailored to support specific missions and relevant security professionals. Moreover, vulnerability assessment reports (VARs) provided critical assessments of physical and operational vulnerabilities at mission buildings. Along with BTAs, VARs were important inputs into risk-based decision-making processes at HQ. Challenges with VAR methodology were acknowledged and improvements to their quality have been noted in recent years (see Finding 15). The Global Security Reporting Program (GSRP) also received DoC funding, which contributed to improving departmental knowledge on relevant strategic issues. Moreover, the Mission Support Initiative provided dedicated intelligence support to missions to ensure that accurate and relevant intelligence was integrated into mission decision-making. In 2022-23, the department officially launched the Threat Assessment Outside Mission Area (TAOMA) project to improve intelligence support to mission staff while travelling.

DoC funding improved the department's threat analysis capacities. A counter-espionage unit was created in 2019-20 and a new analytic cell was established to support the Technical Security Team in 2020-21. The counter-espionage unit worked in collaboration with Canada's security partners to track suspicious incidents across the network and supported high-risk and critical-risk missions on counter-espionage mitigation. Both teams focused on the protection of top-secret information, networks and workspaces; supported security briefings to senior officials; and engaged with the Five Eyes. They contributed to improving the security of information, which enabled decision-makers to access and discuss classified and highly classified information.

Effectiveness

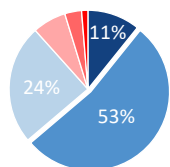
Preparedness to respond and minimize the impact of threats

Pillar 3 of the DoC envelope funded preparedness-focused initiatives such as: providing mission staff with security training and safety and security drills; establishing security-related communication channels and informing staff about local security developments (e.g. security briefings to staff and visitors upon arrival to mission and managing security alert systems); emergency planning; and setting up an alternate command post (ACP).

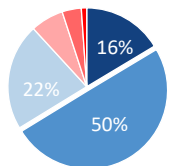
Mission survey results



HQ-led security trainings were identified as the **MOST EFFECTIVE** DoC initiative at addressing mission security needs.



88% of DoC decision-makers at least **somewhat AGREED** that safety and security initiatives contributed to better preparing mission staff to respond to/minimize the impact of threats or incidents (highest ranked out of 5 DoC expected results).



88% of DoC beneficiaries at least **somewhat AGREED** that safety and security initiatives prepared them to respond to risks or incidents at mission (second highest ranked out of 5 DoC expected results).



Finding 7: DoC-funded initiatives that had a deliberate focus on preparedness improved the capacity of mission staff to respond to and minimize the impact of threats and incidents abroad. However, these efforts were inconsistent across the mission network and between different stakeholder groups, including women, LES and 2SLGBTQI+, among others.

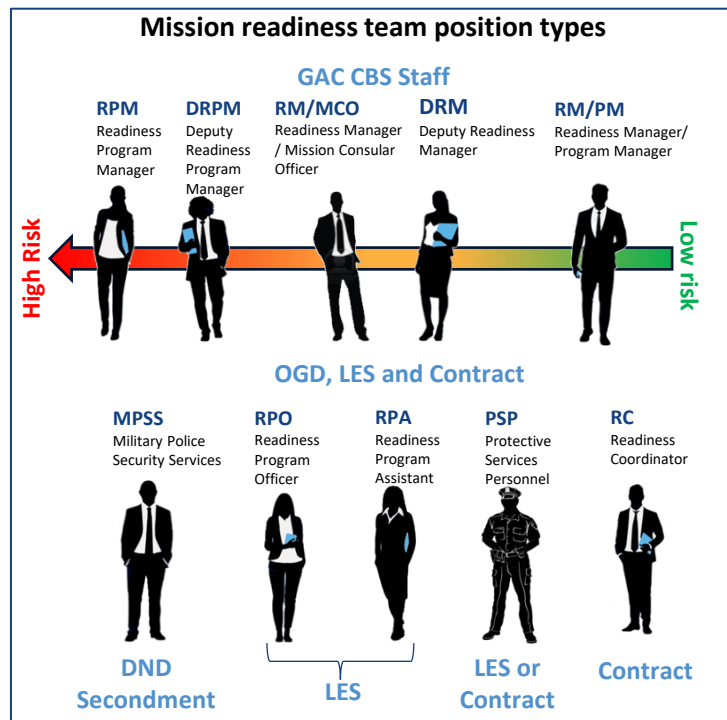
Under Pillar 3, the DoC envelope funded a wide range of safety and security initiatives that had a deliberate focus on mission readiness and preparedness (see sidebar). These initiatives were implemented by both mission readiness teams (see Finding 8) and HQ responsibility centres.

Evidence demonstrated that, when delivered, **preparedness-focused initiatives made a positive difference to improving mission staffs' understanding of threats and vulnerabilities and better prepared them to respond to and/or minimize the impact of threats and incidents at mission** (see survey results in sidebar). However, the **success of these initiatives varied across the network and was dependent on several factors**. Case study evidence highlighted that an inadequate frequency and/or relevance of mission-led training, drills and communication hindered mission staffs' opportunities to build the awareness, knowledge and skills necessary to respond to risks. Additionally, poor participation rates among staff, combined with complacency and compliance issues, hindered their capacity to be responsive. Finally, access to mission-led training and drills varied among different stakeholder groups. There were multiple examples where LES were not included in mission-led initiatives, limiting their level of preparedness compared to their CBS counterparts. In addition, while some OGD staff had already received appropriate training that was perceived as superior to that provided by GAC; many others were under-prepared compared to GAC staff. There were also examples of CBS dependants not being included in readiness drills, alert systems and activities that were relevant to their safety and security needs. Evidence also pointed to a **lack of consistent GBA Plus considerations in security-related briefings, training and drills at mission**. It was well acknowledged that certain groups faced heightened risks while posted or working at Canadian missions (e.g. women, LES, 2SLGBTQI+, people with disabilities, CBS dependants; see Finding 11 for details). However, mission-led initiatives did not always inform or prepare different stakeholder groups for the specific risks they faced, including those related to gender, disabilities, 2SLGBTQI+ and the unique experiences of LES and CBS dependants.

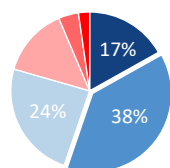
At HQ, the mission readiness support team made significant efforts to enhance mission preparedness by developing standardized readiness tools, templates and checklists aimed to improve the consistency of mission readiness delivery across the network. The DoC envelope also financed HQ-led pre-deployment training such as Hazardous Environment Training (HET) and the Personal Security Seminar (PSS), as well as intelligence-focused security training programs (e.g. Governance, Access, Technical Security and Espionage [GATE]). **Evidence highlighted the effectiveness of these training programs to prepare mission staff and dependants to respond to a range of risks while working and living abroad (see sidebar)**. However, while PSS and HET were mandatory for CBS, they were not always available for LES. The effectiveness of these trainings was hindered by COVID-19 and the resulting lack of access to in-person modules. Concerns were also raised about the real-world applicability of standardized training models given the wide range of security contexts across missions.

Effectiveness

Mission security posture



RPM Capacity



79% of DoC decision-makers at least somewhat **AGREED** that MRTs were sufficiently trained and prepared to support their mission's security posture.

■ Strongly Agree
 ■ Agree
 ■ Somewhat Agree
 ■ Somewhat Disagree
 ■ Disagree
 ■ Strongly Disagree

Since COVID-19, RPM training was reduced from 7 weeks to 4 weeks (2 in-person, 2 virtual). Case study evidence highlighted that this new model was not adequate to prepare new RPMs to deliver on readiness results.

Finding 8: The Mission Readiness Program overall contributed to improving vigilance and strengthening the security posture of missions. However, the success of this initiative varied greatly from mission to mission.

One of the DoC envelope's most important contributions to mission security was the creation of the Mission Readiness Program (MRP). Evidence highlighted that the **MRP strongly contributed to improving mission vigilance and strengthening security posture by reinforcing a mission's "security culture" and establishing networks with in-country security actors.** This involved sustained efforts by the mission readiness team (MRT) to foster: 1) engagement with mission staff (see Finding 7); 2) management buy-in/prioritization of security initiatives; 3) trust and confidence from mission staff in the Readiness Program Manager (RPM)/ Readiness Manager (RM); and 4) strategic outreach with in-country security stakeholders.

Survey and case study evidence demonstrated that **the success of the program varied across the network and was dependent on the MRT's composition and resources, capacity and on team members' personal suitability** relative to the security environment. Finite readiness resources were allocated based on a structured methodology; however, they were not sufficient to meet mission demand, leaving MRTs at many missions understaffed. Staffing RPM positions, especially in high hardship missions, was challenging given the limited pool of qualified and interested candidates. Moreover, **the composition of MRTs (see sidebar for position types) and their capacity (experience, skills, knowledge) varied across missions** (see sidebar on RPM capacity), with implications for a team's ability to build trust and confidence among mission staff. Certain positions demonstrated stronger value compared to others. Both the RPM and Readiness Program Officer (RPO) added significant value to mission security. In addition, having both an RPM and deputy RPM provided higher-risk missions with the capacity to respond to crises while also ensuring the MRT delivered on its regular mandate. While RMs made important contributions to a mission's security posture, they were dedicated to security on a part-time basis and were thus equally occupied by other demanding responsibilities. The effectiveness of Military Police Security Services (MPSS) also varied across missions. The Department of National Defence (DND) managed MPSS deployment and performance management; GAC did not have control over these processes. Evidence demonstrated that some individuals lacked the appropriate attitude and skillset for the role.

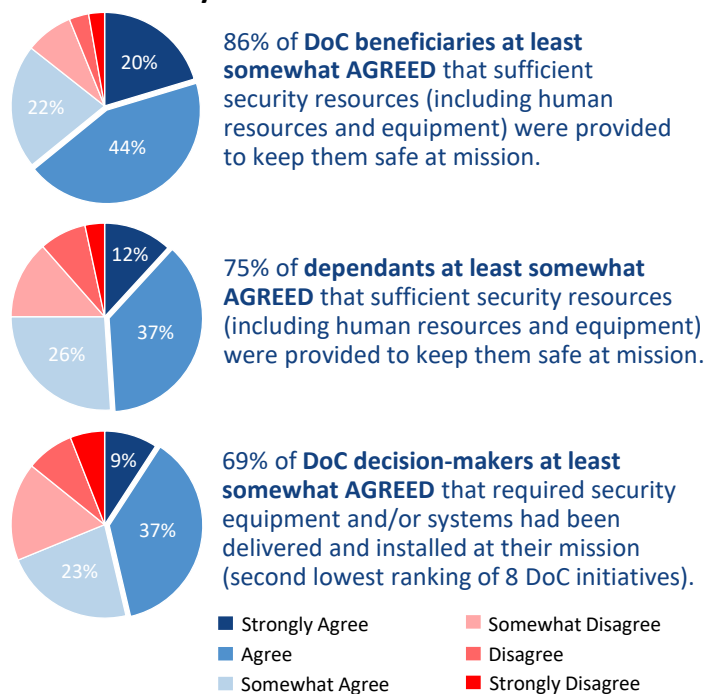
An individual's **personal suitability relative to the demands of the RPM/RM position was another factor for MRT success.** Case studies highlighted that an RPM/RM was considered strong when they were willing to put in the required effort to strengthen the security culture at mission. At some missions, trust and confidence were shaken when the RPM/RM did not effectively manage resources to support mission staff outside of work hours.

Effectiveness

Mission security posture

Pillar 3 of the DoC envelope provided funding for security equipment and systems for missions across the network. This included, but was not limited to, X-ray machines, metal detectors, armoured vehicles, chancery electronic security systems, locksmith services and bullet proof vests. Requests related to closed-circuit television (CCTV) systems were often transferred and managed under minor projects, given their complexity (see Finding 4).

Mission survey results



Finding 9: Delays in equipment and systems delivery hindered missions' readiness and limited their overall security posture.

DoC decision-makers and implementers noted that security equipment and systems were critical for strengthening a mission's state of readiness and reinforcing its security posture relative to its risk environment. However, evidence highlighted **challenges with the procurement process⁷ and timely delivery of equipment and systems to missions across the network**, which limited this initiative's responsiveness to emerging risks and its ability to address mission safety and security needs.

Across the mission network, **31% of DoC decision-makers and implementers did not agree that the required security equipment and systems had been delivered and installed at their missions** (second lowest out of 8). This translates to a substantial number of missions that did not receive critical security equipment in a timely manner to effectively address vulnerabilities, leaving mission staff at risk. While DoC beneficiaries and, to a lesser extent, their dependants reported a more positive view (see sidebar), equipment and systems was ranked as the sixth most effective DoC initiative out of the 8 assessed. Across case studies, evidence showed that certain items were frequently noted as either non-functioning or non-existent. There were multiple examples of requests for equipment that had been in progress for years and mission frustration with the slow response times and opaque prioritization processes (see Finding 15) managed by HQ counterparts. In addition, a lack of GBA Plus considerations when purchasing essential security equipment for staff posted to higher-risk missions negatively affected certain stakeholder groups. For example, women had challenges with the personal protective equipment (PPE) provided (e.g. bullet proof vests, protective gloves, helmets, etc.). PPE was standardized and more appropriately fit a male body, leaving women more vulnerable to physical threats.

One primary challenge that hindered the timely delivery of these items to missions was the procurement process, which often caused delays (see Finding 19 for more details). Evidence pointed to multiple compounding factors, including different requirements in different countries for different goods, a lack of suitable suppliers, low departmental threshold for purchasing goods internally, and a lack of security-specific expertise from OGDs that provided procurement support (see Finding 20). In addition, depending on the nature of the purchase or mission-specific authorities, many missions did not have the authority to procure the needed equipment on their own and were fully reliant on HQ to support them. There was widespread recognition among both case study respondents and HQ interviewees of the need to better understand which elements of the envelope could be effectively delegated to missions for procurement and implementation in order to improve DoC efficiency.

ACM recognized the challenges with planning and delivering equipment and systems and has made concerted efforts to improve service delivery to missions (see Finding 4 for details). However, it is too early to fully assess the impacts that these changes have had on DoC delivery and results.

⁷ The term "procurement process" includes all elements in the procurement/supply chain continuum, including the planning, purchasing, and delivering of goods and services, as well as financial/budget considerations. This process involves multiple responsibility centres within GAC as well as OGDs (when above GAC's authority limits) and is subject to relevant government regulations.

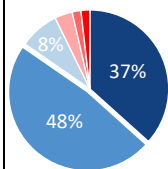
Effectiveness

Mission security posture

Mission survey results



The contracting and deployment of local security guards was identified as the **second MOST EFFECTIVE** DoC initiative at addressing mission security needs.



93% of DoC decision-makers at least **somewhat AGREED** that local security guards were contracted and deployed as needed to support their mission's security posture.

■ Strongly Agree
 ■ Somewhat Agree
 ■ Disagree
■ Agree
 ■ Somewhat Disagree
 ■ Strongly Disagree

As of 2022-23, GAC maintained security guard service arrangements across 140 missions:



92 missions had an individual contract with a private security contractor



37 missions were covered under 12 regionalized contracts



11 missions had an alternative arrangement

Remuneration of local security guards

Evidence highlighted that inadequate guard remuneration was a challenge. HQ teams introduced innovative mechanisms to support better guard remuneration to put more value on service quality rather than cost. However, uneven mission awareness of contracting options and local labour laws were limiting factors.

Finding 10: Local security guards were an important initiative to maintain mission security posture, however, challenges in managing security guard contracts limited the strength of this DoC initiative;

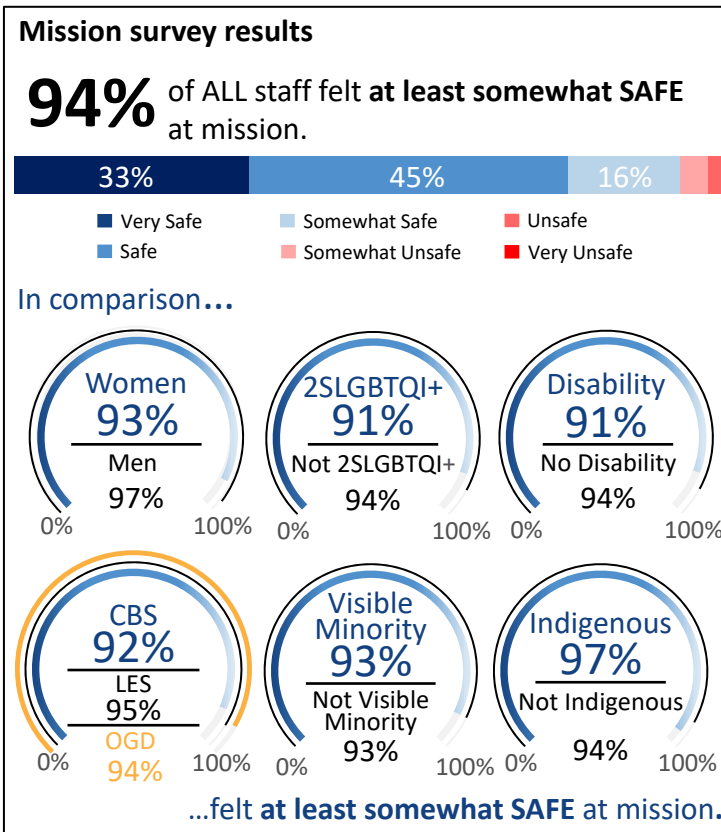
DoC funding under Pillar 3 provided the department with financial resources to contract local security guards at missions abroad (see sidebar for details). Outsourcing security guard services was generally consistent with practices employed by other allies and worked well under stable conditions. Survey evidence highlighted the importance and effectiveness of local security guards for a mission's overall security posture, with **over 40% of DoC decision-makers and implementers ranking this initiative as the most effective at addressing mission security needs** (second highest ranking after HQ-led security training – see sidebar).

However, case study evidence, best practices from the environmental scan, and interviews pointed to **the need for sustained efforts by the readiness team to effectively oversee and manage guard contracts**. This included paying greater attention to contractor practices in the selection and treatment of guards, as well as ensuring training and maintenance of skills. Evidence also pointed to challenges with adequate remuneration and ensuring that contracts represented the best value (in terms of security protection) rather than the lowest cost (see sidebar). Case study evidence identified examples where the effectiveness of local security guards in strengthening a mission's security posture varied. Respondents at some missions reported that **underpaid, undertrained and/or overworked guards did not build trust and confidence among mission staff**. For example, respondents confirmed that some guards were caught or suspected of stealing from staff quarters (SQs) or were found sleeping at SQs while on active duty and were therefore unresponsive to staff urgencies. Unsustainably long stretches of continuous work and/or inadequate remuneration were noted as the primary drivers of inappropriate conduct; the former constituting a breach of contract by the contracted firm.

According to interviews, **HQ supported missions with dedicated resources throughout the local guard contracting process**. Since 2017, sustained efforts have been made to establish a centre of expertise at HQ focused on improving the standardized guard contract, providing in-person and online training to local security guards, and providing direct support to missions to review contract compliance issues. That said, once a guard contract was in place, the quality of guard services was dependent on the mission readiness teams' capacity to ensure that contracted firms respected contractual obligations, which varied across the network (see Finding 8). Case study evidence highlighted examples of readiness teams working diligently to improve the quality of guard services. In one successful case, interviewees reported a dramatic improvement to guard quality that resulted from the readiness team's specific efforts to renew and improve the guard contract. The team also established a culture of loyalty by creating a system of appreciation and recognition that incentivized a stronger work ethic and further improved the quality of guard services. In other case studies, there have been concerted efforts to improve the gender balance in security guard services. For example, in one case study, guard contracts purposefully included provisions for increased female guard and close protection officer representation. In this case, this reflected an improvement to security guards' ability to understand and respond to gender-specific issues.

Effectiveness

GBA Plus



DoC for LES and contractors

While the department owes a legal DoC to LES and contractors (see p.17), evidence pointed to a lack of clarity among stakeholders on the department's specific legal DoC responsibilities in relation to these groups. During times of crisis, this could result in increased risks to these stakeholder groups given the uncertainty regarding the standard of care that they may or may not receive under certain circumstances.

Finding 11: While all demographics generally reported feeling safe or very safe at mission, the multiple stakeholder groups across the mission network experienced differences in the risks they faced.

Overall, mission survey respondents' perception of their individual safety at mission and/or in their current living situation abroad was positive. **Approximately 94% of mission staff indicated that they felt at least somewhat safe at their current mission** (see disaggregated survey results in sidebar). At the aggregate level, the survey did not identify significant variances in the reported feelings of safety by equity-deserving groups (women, persons with disabilities, 2SLGBTQI+ persons, visible minorities, and Indigenous peoples). However, one noticeable difference was that only 88% of CBS dependants reported feeling at least somewhat safe, which was significantly lower than the responses from mission staff. Another stark difference in perception was that only 75% of survey respondents who identified as having disabilities agreed that safety and security initiatives delivered by the government had improved the overall safety of all people at mission (compared to 88% of respondents who did not identify as having a disability).

Furthermore, case study evidence demonstrated that **stakeholder groups at mission experienced differences in the risks they faced**. While LES often had a higher baseline level of comfort in the country-of-mission operation, they reported experiencing unique risks that were not well addressed through DoC investments. For example, case study evidence highlighted that some LES were targeted by individuals in the community outside of their work hours and were pressured to provide information or services as a direct result of their employment with the Canadian embassy. LES reported that these encounters ranged from innocuous but uncomfortable conversations to more persistent and aggressive verbal harassment.

Moreover, across case studies, women were more likely to raise the concern of gender-based violence and harassment outside of work hours compared to their male counterparts at mission. Within the wide range of countries and contexts that Canadian missions operate, women often faced disproportionate risks relating to violent and sexual crimes. Additionally, having one or more disabilities was recognized as an increased risk factor, in particular due to barriers that affect mobility, both in and outside mission buildings. CBS who identified as part of the 2SLGBTQI+ community also faced unique threats that their other mission colleagues did not. In some countries, people belonging to 2SLGBTQI+ communities experience higher levels of homophobia and discrimination, which can elevate the risk of assault and other violent crimes.

CBS dependants mentioned additional risks that were grounded in language barriers. Without access to the same language training offered to CBS, dependants reported an inability to navigate sensitive or uncomfortable situations, which increased their overall vulnerability. Case study evidence highlighted the common sentiment that there was a lack of consistent GBA Plus considerations in DoC envelope planning and implementation. This created a challenge given the diverse cadre of employees and dependants at mission.

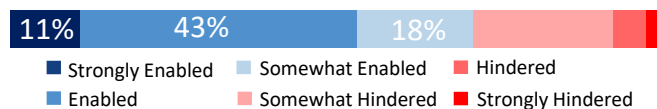
Finally, evidence pointed to a lack of clarity regarding the extent of safety and security coverage for different stakeholder groups at mission (see sidebar).

Effectiveness

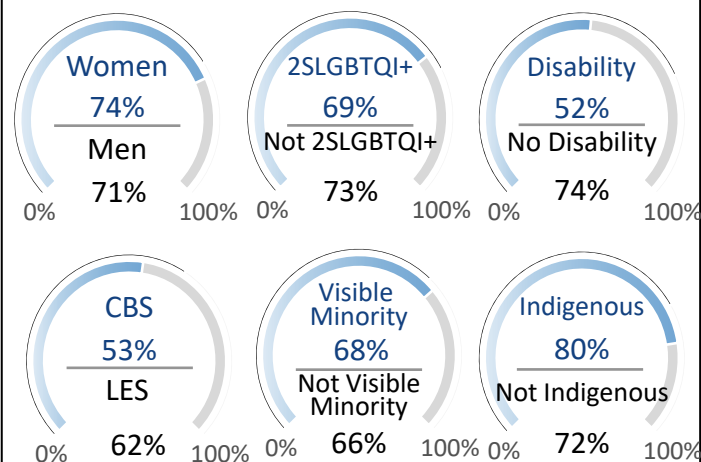
Maintaining business operations

Mission survey results

71% of ALL staff felt that safety and security initiatives at least somewhat **ENABLED** their ability to do their work effectively.



In comparison...



...felt that safety and security initiatives at least somewhat **ENABLED** their ability to do their work effectively.

Note: not all respondents answered each question, the percentages shown above are calculated based on the total number of respondents for each demographic category.

Finding 12: Security protocols could hinder staffs' ability to deliver programming if they were unjustifiably restrictive and not sufficiently informed by evidence. Restrictions were generally welcomed in higher-threat environments.

While DoC-funded initiatives were put in place to protect CBS, LES, CBS dependants and visitors to missions abroad, evidence from case studies and the mission survey (see sidebar) revealed that **security protocols could negatively affect mission staffs' ability to do their work effectively to deliver on GAC's international priorities**. While 71% of survey respondents agreed that safety and security initiatives at least somewhat enabled their ability to work effectively, a significant percentage (29%) reported that the initiatives at least somewhat hindered their ability to work effectively.

The effect that DoC had on survey respondents' ability to do their work varied significantly across different groups at mission (see sidebar). DoC decision-makers were one of the most positive groups overall, with 76% considering these initiatives as an enabling factor. On the other hand, CBS were highly critical, with only 53% reporting that safety and security initiatives allowed them to do their work effectively. Across mission hardship levels, respondents located in high hardship missions rated the safety and security initiatives as the least enabling. Further insights from a GBA Plus lens revealed that women were overall more positive than both men and the average respondent. However, respondents that self-identified as a person with one or more disabilities were the most critical group overall with only 52% indicating that DoC was at least somewhat enabling. 2SLGBTQI+ and CBS who identified as a visible minority were more positive, but still more critical than the average mission staff. Indigenous peoples were by far the most positive group, with 80% reporting DoC as an enabling factor (see sidebar for details).

Case studies identified **examples that help explain the negative sentiments that surfaced from the survey**. In some cases, restrictive travel protocols hindered the advancement of Canadian priorities in a particular country or region and were challenged by some CBS staff. They felt that travel restrictions impeded their ability to engage local community stakeholders and effectively manage the programming that fell under their team's specific mandate, which often required travelling to higher-risk regions where GAC was operating.

Restrictive policies were often attributed to an **RPM's low risk tolerance and/or a lack of evidence about the threat environment**, in addition to a lack of rigorous and transparent research and analysis to inform decision-making (see Finding 8). While there was a constant trade-off between security protocols and maintaining business operations, transparent and evidence-based decisions by the readiness team were found to improve the acceptance and understanding of security-related decisions by mission staff. **Restrictive travel protocols in higher-risk case study missions were generally well-received by mission staff and contributed to their confidence in mission security teams.**

Findings: Efficiency and coherence

Efficiency and coherence

Roles, responsibilities and accountabilities



Source: 2019-20 DSP

Mission Security Risk Model (MSRM)



Finding 13: Specific structures, processes and mechanisms were leveraged and built into the envelope's design to facilitate a responsive, risk-based approach to managing finite departmental security resources.

Since 2017, GAC has leveraged, developed and integrated a number of **structures, systems and processes to facilitate a robust, responsive and risk-based approach to addressing security vulnerabilities and mitigating threats at missions across the network**. Pre-dating the DoC envelope, the **Departmental Security Plan (DSP)** provided GAC senior management with integrated plans focused on delivering effective security programming across the department. Building off this, and in response to the recommendations of the *2016 Evaluation of Mission Security and Personal Safety Abroad*, the department developed the **Global Security Framework (GSF)** to facilitate effective and efficient governance of the department's finite security resources, grounded in the concept of evidence-based decision-making (see sidebar). Under the GSF, The **Security Management and Governance Framework (SMGF)** provided a high-level overview of the department's security structure, responsibilities, accountabilities and governance (see Annex X). Furthermore, the **Departmental Security and Investment Plan (DSIP)** was designed as an "integrated planning tool to ensure the department employed a robust, risk-based approach to addressing security vulnerabilities and mitigating threats at missions" (2021-22 to 2026-27 DSIP; see Annex XI). Approved DoC-funded initiatives were then monitored through the **DSP implementation matrix**. The **Mission Security Risk Model (MSRM)** was intended to inform decision-making on DoC investments based on risk and prioritization.⁸ Risk was calculated based on an assessment of assets, threats and vulnerabilities (see sidebar).

The DoC governance framework was also supported by processes and mechanisms intended to ensure that shifting global risks could be identified, responded to and mitigated in a timely fashion. These included the annual and mid-year review of the DSIP as well as the **pressure/reallocation mechanism**. Pressures and reallocations were defined as unforeseen investment requests brought on by events and ongoing situations facing Canadian missions abroad. Branches submitted funding requests for governance approval (see Annex IV) at the annual DSIP planning exercise or during the mid-year review. New requests that were deemed urgent were considered under the exceptional approval process. To be considered for approval under the DoC governance framework, the funding requests had to: 1) be within the DoC envelope scope and aligned with 1 of the DoC pillars; 2) serve to mitigate a defined risk (financial and/or security-related risks); and 3) be deemed necessary in consideration of the requesting branch's existing DoC resource levels. Evaluation evidence highlighted that **the design of these elements aligned with the department's security mandate** to deliver responsive, risk-based safety and security programming to GAC missions. **Assessments of how well they performed throughout DoC implementation are provided in subsequent findings.**

⁸The GSF, DSIP and MSRM were all directly built into the DoC envelope design as per the 2017 TB submission.

Efficiency and coherence

Roles, responsibilities & accountabilities

DoC HQ responsibility centres

International Platform (ACM)
Designs and delivers major and minor physical security projects and security equipment and systems; manages guard contracting, MPSS salary and common services for MRTs.
Consular, Security, Emergency Management (CFM)
Conducts VARs, allocates and trains MRT positions, oversees regional emergency management offices (REMOs), provides mission support, serves as the DoC security committee secretariat, co-chairs SIPAB and the ADM Oversight Committee. The chief security officer responsibilities reside within CFM.
People and Talent Management (HCM)
Ensures occupational health and safety, produces health policy and analysis, responds to health incidents and medical emergencies at missions abroad.
International Security and Political Affairs (IFM)
Produces security intelligence reporting (including BTAs and TAOMAs), analyzes and mitigates technical security threats, is responsible for highly classified systems and information, conducts GATE training.
Corporate Planning, Finance, and IT (SCM)
Houses the corporate planning and finance functions, leads on network improvements and cybersecurity, is responsible for unclassified and classified systems and information.

⁹ Multiple departmental studies (e.g. 2016 Evaluation of Mission Security, 2018 OAG Audit) noted deficiencies with respect to the clarity of roles, responsibilities and accountabilities and made recommendations to better define them.

Finding 14: The complex DoC delivery structure and the lack of a clear and comprehensive departmental security policy or directive resulted in blurred accountabilities, roles and responsibilities, and led to inefficiencies and challenges in coordination and collaboration.

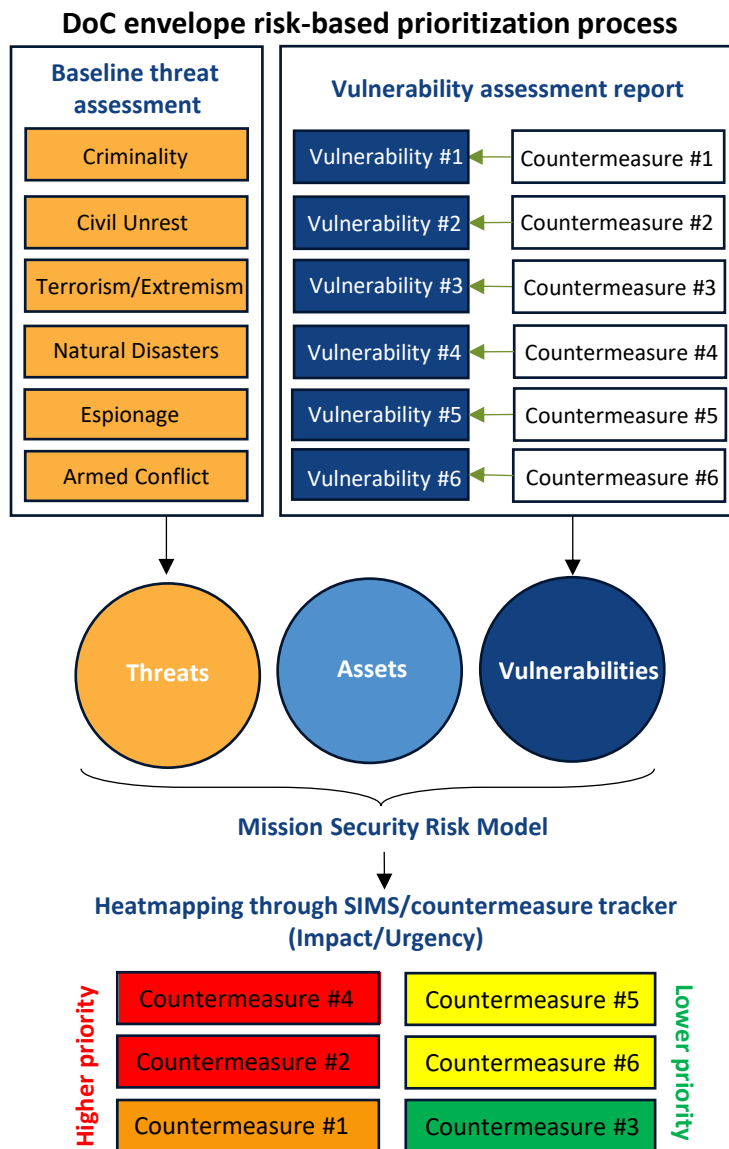
DoC stakeholders included multiple bureaus, divisions and units within ACM, CFM, HCM, IFM, SCM (see sidebar and Annex III), geographical branches, and mission staff and management across the network. **Elements of DoC planning and delivery were shared, divided and often siloed among these stakeholder groups, resulting in blurred roles, responsibilities and accountabilities.**⁹ Evidence highlighted that management had a good understanding of the high-level roles and responsibilities in the Security Management and Governance Framework (see Annex X) and of HOMs' accountabilities, but this understanding decreased at the working level. Furthermore, closely related functions were split across or within branches, leading to duplication and inefficiencies in the absence of efficient collaboration mechanisms. The evaluation period also saw changes in the chief security officer (CSO) role, which was originally performed at the level of ADM and was later designated to a single director general (DG) in 2019. In 2021, CSO responsibilities were split across 2 DG functional areas within CFM.

While the DoC envelope included new security-focused governance structures under the GSF (see Finding 13), **GAC did not have a clear, comprehensive and actionable departmental security policy or directive.** Evidence revealed this as a significant institutional gap, **leading to a lack of clear accountability and ownership**, including for residual risk. While the Manual of Security Instructions (MSI, 2015) identified policy statements and standards to meet the requirements in the TB *Policy on Government Security*, it pre-dated the DoC envelope by 2 years and no longer reflected current roles and responsibilities. Moreover, overarching financial oversight for the DoC envelope was not well understood; each branch was accountable for its own spending, leaving gaps in oversight during implementation and ultimate accountability.

The DoC's complex organizational structure required a significant level of coordination, communication and collaboration. **However, this proved challenging given the lack of clarity on roles and responsibilities, the absence of a comprehensive security policy and other impediments.** The latter included a lack of compatible tracking tools (Finding 17), divergent internal priorities and planning processes (Finding 15), and a lack of security culture across the department. At the mission level, missions were involved in the HQ-led vulnerability assessment process but were insufficiently consulted and informed about project progress and other DoC activities affecting them (e.g. training requirements). Efforts to address these challenges have recently been implemented through changes in senior leadership positions, the introduction of new coordination roles and tools (including pilot initiatives delegating authority to missions to implement physical security enhancement projects) and an increased focus on the highest priority missions.

Efficiency and coherence

Risk-based prioritization



Finding 15: The prioritization of DoC funding and programming was limited by the envelope’s complexity, the number and variety of stakeholders involved, competing priorities, and reliance on outdated systems, processes and tools.

Risk-based prioritization was well documented as a fundamental component of GAC’s security programming to ensure that resources were effectively allocated to address the most pressing safety and security priorities across the mission network. To this end, and in response to the recommendations from the 2016 mission security evaluation, the department developed the Departmental Security and Investment Plan (DSIP) (see Finding 13 and Annex XI). However, **its implementation was limited by several shortcomings. DoC risk-based prioritization processes involved multiple responsibility centres across the department.** This created **diverging priorities, requiring trade-offs between effective security risk mitigation, fulfilling operational requirements and practicalities for project delivery**, including feasibility and the availability of DoC resources.

One important example of how different departmental priorities affected prioritization was the original selection of 26 major capital projects in the 2017 DoC TB submission. Based on an analysis of missions’ vulnerability assessment reports and risk assessments, the evaluation found that multiple locations selected for the 26 original major capital projects did not represent the highest priorities for addressing vulnerabilities when compared to alternative missions that were not selected. Respondents also noted that the original selection of some projects did not necessarily align with a risk-based prioritization approach.

Moreover, while the risk-based prioritization process for mission risk mitigation was logical and systematic (see sidebar), its strength was **limited by the inconsistent quality and timeliness of threat and vulnerability inputs** (baseline threat assessments and vulnerability assessment reports), **weaknesses in risk assessment methodologies** (including for assessing residual risk), and **reliance on systems and tools** (e.g. SIMS, MSRM, countermeasure tracker) that were reported to be outdated and did not support communication across responsibility centres.

Additionally, there was evidence that **CFM and ACM faced challenges in agreeing on a single, prioritized list of physical vulnerability mitigation measures to be implemented at missions.** The process of reconciling security priorities with project management priorities was complex and had not yet been resolved at the time of the evaluation. Challenges with minor project tracking and reporting also compounded this issue given the lack of integration between each branch’s primary tracking systems (see Finding 17).

Despite the challenges, the **responsible stakeholders demonstrated a high level of awareness and worked to address these various shortcomings.** The threat assessment team identified improvements to the content and format of BTA products and VAR methodology has improved (see Finding 6). The mission readiness and security operations team has also been working toward adopting risk assessment tools that better meet industry standards (the harmonized threat, vulnerability, risk assessment framework and analytical software for threat assessment). CFM and ACM have implemented several measures to de-conflict priorities and increase collaborative prioritization efforts.

Efficiency and coherence

Governance

ADM DoC Oversight Committee

- ADM-level committee
- reviews and endorses the multi-year DSIP recommended by SECCOM and refers it to the deputy head (USS) for final approval
- reviews and approves DoC pressures and re-allocations referred and endorsed by the SIPAB and SECCOM that exceed \$10M

Security Committee (SECCOM)

- DG-level committee on security (not exclusively DoC)
- 2 rotating ADM chairs
- provides oversight, strategic guidance, and/or approval of the DSP, DSIP and DoC envelope initiatives
- reviews, endorses and approves DoC pressures and reallocations referred and endorsed by SIPAB up to its pre-established threshold

Security Investment Planning Advisory Board (SIPAB)

- director-level committee
- 2 DG chairs
- integrates and prioritizes security investments between/across DoC envelope funding streams
- coordinates subject matter expert input into the DSIP and submits it to SECCOM
- monitors DoC-funded initiatives and reviews, endorses, or approves pressures and reallocations based on its pre-established threshold

Finding 16: The DoC governance structure enabled a timely allocation of funding and was responsive to emerging needs and crises but did not sufficiently fulfill its challenge function.

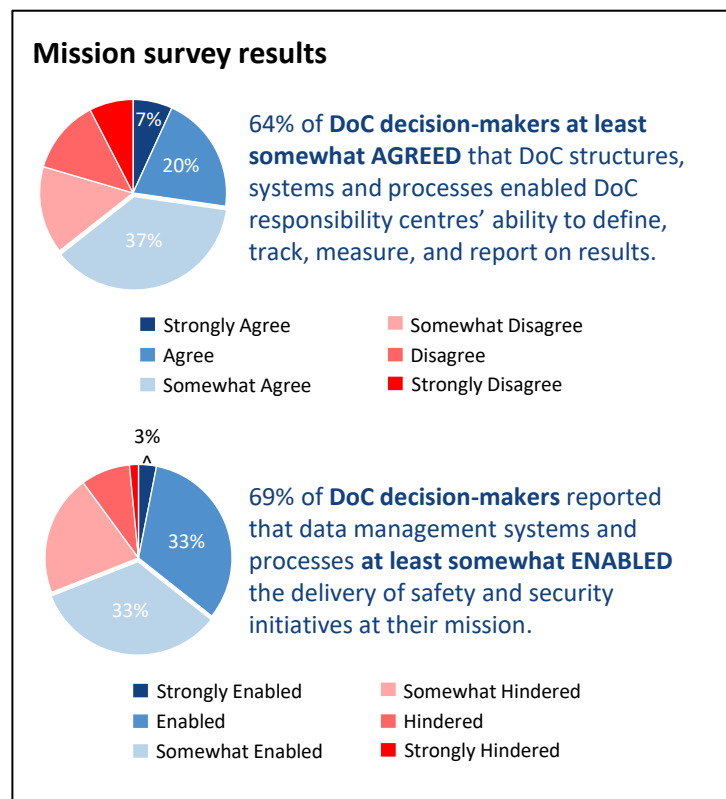
The DoC envelope had a built-in governance structure (see sidebar and Annex IV) with specific mechanisms intended to ensure that security investment planning was integrated across program streams within the department and that shifting risks affecting missions could be responded to in a timely fashion (see Finding 13). Evidence demonstrated that the **governance structure enabled agile and responsive allocation of DoC funding**, which allowed the department to reallocate unspent funds and fund pressures in response to off-cycle security requests, some of which arose from crisis situations such as in KABUL and KYIV. However, multiple lines of evidence from the evaluation revealed that **funding allocation was not stringently prioritized based on risk during the evaluation period**, pointing to challenges with the governance function.

The Security Investment Planning Advisory Board (SIPAB) was responsible for reviewing GAC's security investment plans (including pressures and reallocations) and for facilitating integration and prioritization of these investments between and across funding streams in accordance with the GSF. However, **there was a lack of clarity on the SIPAB's roles, responsibilities and accountabilities, as well as structural and process issues** that limited its challenge function in the early years of DoC implementation. The envelope required subject matter expertise to review proposed investments from various program streams – expertise that board members did not always have and, as a result, made them feel ill-equipped to challenge funding proposals. There was also pressure in the early years to spend money and avoid lapses. The ratio of available budget to the number of projects at the envelope's onset allowed decision-makers to approve most new pressures and reallocations without having to assert a rigorous challenge function. For example, of pressures submitted by October 2022, SIPAB approved all (\$182M) "critical" and "high" pressures and also nearly all (\$27M) "medium" or "low" pressures. As the envelope's financial situation changed at the mid-way point in DoC implementation, fewer resources were available to respond to future crises. **This has placed greater demand on DoC governance to prioritize investments in the remaining years of implementation.**

Internal reviews in 2021 of DoC governance noted opportunities to clarify accountabilities across the various committees and to improve their focus on monitoring performance. **Improvements were recently made to address these identified challenges.** In 2022-23, SIPAB's terms of reference were amended to enhance the board's capacity to fulfill its mandate and provide greater oversight of performance monitoring. This included an expanded mandate, the adoption of measures to improve committee independence, new co-chairs, and an overhaul of membership that incorporated representation from 2 geographic branches and HCM. However, at the time of the evaluation, it was too early to fully assess the impacts that these changes have had on DoC delivery and results.

Efficiency and coherence

Tracking and reporting



Finding 17: Tracking and reporting on DoC progress and results were not sufficiently robust to support evidence-based decision-making.

The 2018 Auditor General's audit on mission physical security documented gaps in the department's ability to track security requirements and report on the implementation of security measures. In response, GAC committed to implementing improvements in monitoring and reporting practices; however, multiple lines of evaluation evidence pointed to **ongoing challenges with the quality of reporting inputs (data), outputs (reports) and supporting tools and systems** that hindered tracking and reporting progress on DoC implementation and results. More than 1 out of 3 surveyed DoC decision-makers and implementers did not agree that the available structures, systems and process enabled the department's ability to define, track, measure and report on DoC envelope results (see sidebar).

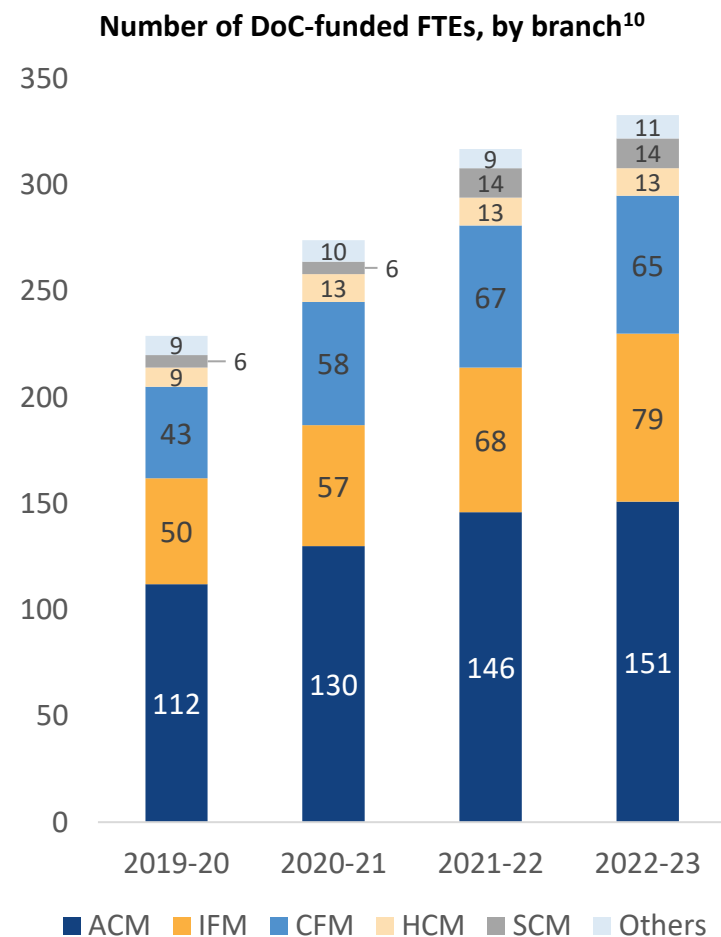
Performance indicators in the DoC annual report's Security Performance Measurement Framework (SPMF) focused primarily on implemented activities and outputs and could not be used to measure progress towards the achievement of DoC results. Interviewees highlighted that the ways in which DoC activities were tracked and measured could only indicate what was done, but not how well it was done, or what result it achieved. Some indicators in the SPMF changed year over year and lacked clear targets and measurement methodologies, limiting the comparability of data over time. Performance information was managed by individual teams and reflected team-specific terms and definitions, which caused confusion when communicating across teams and led to discrepancies in the annual report. Interviewees specifically identified a need to critically reassess DoC performance measurement practices to better align it with targeted results.

Databases and tools used to track individual DoC initiatives required significant manual efforts to keep them up to date, which proved challenging. For example, tracking progress for minor projects, equipment and systems required inputs, communication and coordination across siloed responsibility centres as well as the use of both classified and unclassified systems. Evidence highlighted that the primary security vulnerability mitigation data repository (SIMS and the countermeasure tracker) often included duplicate entries as well as outdated requests and mitigation strategies in relation to identified security requirements. Reporting on physical security projects was also compartmentalized across classified and unclassified systems for security purposes and used broad definitions (e.g. "on track") that did not provide stakeholders with visibility into project status. The lack of updates when specific security requests were actioned or completed caused further confusion and ultimately hindered evidence-based decision-making and prioritization efforts for these funding streams. As of 2023-24, ACM established the service delivery portal (SDP) as the exclusive platform within the branch to improve tracking and reporting on SLPs, including by increasing access to key stakeholders (both at HQ and mission).

Evidence also pointed to challenges with tracking and reporting for mandatory training (HET/PSS). With mission staff rotations and no centralized records of certification and expiry dates for CBS and their dependants, it was difficult to track employee training completion rates.

Efficiency and coherence

Human resources



¹⁰The data captures FTE positions as of March for each FY from 2019-20 to 2022-23. "Other" includes EGM, OGM, NGM, WGM, ZID and pools roll-up; each had 3 or fewer FTEs funded by the DoC envelope per year. FTE data for 2017-18 and 2018-19 were not available.

Finding 18: Multiple interrelated human resources challenges hindered the timeliness and responsiveness of the delivery of DoC initiatives.

The DoC envelope funded over 330 full-time equivalent (FTE) positions to support the delivery of its initiatives. The onboarding of funded FTEs was gradual, with some positions requested through TB submissions and others through ongoing reviews of pressure submissions. The majority (89%) of funded FTEs were concentrated in ACM, CFM and IFM and addressed important gaps identified by the branches.

Despite increases in the number of positions, evaluation evidence identified **various challenges related to human resource availability, composition and capacity that negatively impacted the timeliness and responsiveness of DoC delivery**. Interviewed HQ stakeholders noted that decisions on the creation of new positions had been made based on the strength of individual funding requests rather than a holistic view of envelope requirements and interdependencies across teams and branches. This resulted in some teams being unable to cope with an increased volume of requests. Clear examples of understaffed teams relative to their DoC responsibilities were those involved in minor project planning and delivery and the Mission Readiness & Security Operations team.

Other difficulties concerned staff recruitment and retention, with several key teams relying significantly on short-term staffing options, which led to gaps in corporate memory and limited investment in training. Various HQ teams reported delayed onboarding of new resources due to GAC's long timeframes associated with position creation and staffing processes, as well as limited classification options for technical and specialized resources. This posed difficulties in light of opportunities available in the private sector and other federal organizations that offered competitive and faster employment, at times without language requirements. The delay in increasing staffing levels under the DoC envelope echoed similar challenges noted in the 2016 evaluation on mission security.

Finally, interviews and case studies provided examples where **insufficient investment in staff training and professionalization** across all subject matter areas negatively impacted the delivery of DoC activities, including for surge support in times of crisis. At missions, case study evidence highlighted significant variations in human resources capacity in relation to mission security. Some missions had limited security-focused human resources both in number and quality, relative to their risk environment, which hindered effective and responsive delivery of DoC activities. Other missions provided examples where exceptional human resource capacity was instrumental in achieving DoC-targeted outcomes abroad (see Finding 8).

Efficiency and coherence

Procurement processes

GAC contracting authorities

Basic contracting limits

- \$3.75M for competitive/\$200K for non-competitive **services contracts**
- \$400K for competitive/\$40K for non-competitive **goods contracts**¹¹
- \$750K for competitive/\$100K for non-competitive **construction contracts**¹²

Exceptional contracting limits

- Competitive **construction contracts** up to: \$2.25M for staff quarters; \$6.75M for official residence; \$22.5M for chancery; \$22.5M for multiple-unit facilities
- \$3M for competitive/\$225K for non-competitive **architecture and engineering services**
- \$11M for competitive **security services contract** for Canadian missions abroad (until Oct 2027)

Emergency contracting limits

- \$1M in response to a **pressing emergency**
- \$15M for non-competitive services contract related to **chanceries or national security-related threats** to Canadian missions abroad

Source: TB Directive on the Management of Procurement, 2024

¹¹ Authorities are for the purchase of goods from suppliers located in the vicinity of mission offices abroad when such procurement action is deemed to be the most practical and economical approach (Source: Delegation of Financial signing Authority – Accompanying Notes, updated 2024).

¹² These limits only apply to construction abroad as GAC does not own property in Canada.

Finding 19: Procurement processes and gaps in capacity contributed to delays in the delivery of DoC equipment, services and projects.

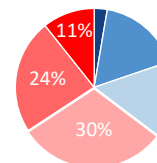
Surveyed DoC decision-makers and implementers at missions identified **procurement as the most significant factor hindering the delivery of safety and security initiatives at mission** (see Annex IX). This view was shared by HQ interviewees, who ranked procurement processes in the top 3 DoC implementation challenges.

Departmental contracting authority levels required that federal common service providers be involved in the procurement of safety and security goods and services above certain thresholds (see sidebar). However, interviewees reported that their **relationships with Public Services and Procurement Canada (PSPC) and Shared Services Canada (SSC) were challenging**, as these departments were limited in their capacity to prioritize and address GAC's time-sensitive requirements for specialized security products in an international context. To better support GAC's internal procurement function, the department was granted an increased authority of up to \$11M for competitive security services contract for missions abroad until October 2027.

Procurement processes within departmental authorities were also challenging, and timelines were lengthy due to difficulties in defining requirements, a disconnection between procurement and planning processes, inventory management challenges, a lack of diversification of delivery methods and suppliers (particularly for high-risk and conflict-affected locations) and variable capacity to leverage the national security exception. Procurement and supply chain-related challenges for X-ray equipment, CCTV cameras, personal protective equipment and armoured vehicles led to unmet mission needs and increased mission vulnerability, often taking years to resolve (see Finding 9). Interviews and the document review identified that the effective procurement of security goods and services for high-risk missions required careful and flexible management of the contracting process, including detailed documentation of all applicable requirements and safeguards to ensure continued performance and use of assessment criteria that placed greater value on quality. The 2021 parliamentary committee report on ensuring robust security in federal purchasing reiterated the importance of considering value and qualifications, rather than focusing on the lowest price.

Mission survey results

- Strongly Enabled
- Enabled
- Somewhat Enabled
- Somewhat Hindered
- Hindered
- Strongly Hindered



65% of DoC decision-makers reported procurement as a factor that **at least somewhat HINDERED** the delivery of safety and security initiatives (highest rated hindering factor out of 10)

Efficiency and coherence

Coordination with federal partners

OGD services to support DoC envelope delivery

OGD	Services provided
National Defence (DND)	Provides and trains MPSS, supports general mission security posture and emergency response for select mission locations and provides limited close protection services.
Health Canada (HC)	Provides medical advice on foreign service directives and undertakes health assessments based on occupational health requirements.
Shared Services Canada (SSC)	Provides digital infrastructure, IT services and procurement related to cyber and IT security and cloud services.
Public Services and Procurement Canada (PSPC)	Acts as a central purchasing agent for procurement above GAC's contracting limits. PSPC also provides security vetting services for individuals and vendors providing services to Canada.

Finding 20: Divergent priorities and capacity limitations among federal partners to support the implementation of some DoC initiatives put pressure on envelope resources and led to gaps in GAC's ability to ensure the protection of staff, information and assets abroad.

In 2022-23, GAC's mission network hosted over 800 positions staffed from other government departments (OGDs) and agencies. GAC also relied on several of these OGDs and agencies to deliver on its DoC envelope responsibilities for missions abroad (e.g. DND for close protection teams in high-risk locations, Health Canada (HC) for health support, PSPC for procurement, SSC for IT). However, these **federal common service providers were limited in their capacity to prioritize and address GAC requirements for specialized solutions in an international context that led to delays and inefficiencies in DoC delivery** (see Finding 19).

In addition, **some federal partners have scaled down support to GAC in recent years** due to capacity limitations and their priorities to re-focus on their core mandates. For example, in 2013 a memorandum of understanding was signed between HC and GAC for the delivery of health services to CBS and their dependants while posted abroad. However, in January 2022, HC withdrew most of these services, stating that overseas support was not part of its core mandate. The scaled-down services provided by federal partners were absorbed by GAC through contracted means and internal resources under the DoC envelope, but their scope and quality were perceived as not always adequate, and their impact was felt more acutely in higher-risk locations (see Finding 3 related to gaps in coverage for health safety and well-being).

There were some examples of good cooperation on specific technical issues with partners (e.g. cooperation with National Research Council Canada on the physical security research program, with DND on cold chain logistics, with SSC on some IT solutions (including bandwidth upgrades) and intelligence sharing with federal partners). However, the whole-of-government approach to ensuring DoC envelope delivery was diminished over the evaluation period.

Conclusions

Conclusions

Design

The DoC envelope marked an important evolution in the department's approach to mission security. It provided GAC with unprecedented resources, increased visibility and trust as the lead security agency to ensure the safety and security of missions and their people across the network through investments in physical infrastructure, information security and mission readiness. The envelope was designed to comprehensively address cross-mission safety and security needs based on 3 foundational concepts: risk-based prioritization, evidence-based decision-making and the capacity to respond to emerging risks. This design and the corresponding initiatives funded through DoC TB submissions were overall well aligned with the department's security mandate and safety and security priorities, including those identified by key mission stakeholders themselves.

However, the evaluation found unaddressed risks across the mission network and among different stakeholder groups. Mission staff felt underserved by departmental resources in the area of health, safety and well-being. Though the original envelope's design did not include references to "health" or "well-being", naming the funding envelope "Duty of Care" led to persistent confusion among DoC responsibility centres and mission staff. It was unclear to them as to whether health, safety and well-being should be considered within the scope of the envelope, in particular given the broader legal DoC implications.

Delivery

The evaluation highlighted several external and internal factors that affected DoC delivery. COVID-19 and the resulting operational difficulties hindered DoC delivery on many fronts. Due to travel restrictions and the negative impacts on global economic conditions (supply chain, inflation and rising costs), DoC-funded initiatives were often delayed, cancelled, and/or otherwise negatively impacted.

The evaluation also highlighted challenges with the envelope's internal structures, systems, processes and tools during implementation. The complex DoC delivery structure and the lack of a clear and comprehensive departmental security policy or directive resulted in blurred accountabilities, roles and responsibilities and led

to inefficiencies and challenges in coordination and collaboration among DoC responsibility centres. In addition, there was evidence of challenges with the envelope's prioritization of DoC funding and programming. The main issues were a reliance on outdated systems, processes and tools; diverging priorities across the department; and the limited challenge function provided by DoC governance. Other challenges were related to tracking and reporting, human resources and procurement processes. Responsible DoC stakeholders demonstrated a high level of awareness and worked to address these various shortcomings. As a result, DoC delivery gradually improved over the first 5 years of implementation.

Results

Despite the challenges, evidence highlighted that the envelope made progress in improving the safety and security of CBS, their dependants, LES (while on duty) and visitors to Canadian missions. However, results varied widely across investment streams and between missions. One of the DoC envelope's most important contributions to mission security was the creation of the Mission Readiness Program (MRP), which made a strong positive difference to improving mission vigilance and strengthening mission security posture. However, the success of the MRP varied across the network and was critically dependent on the composition and resources of each readiness team, as well as their capacity and personal suitability. Evidence also showed that DoC initiatives helped strengthen the security and resilience of missions' unclassified network and maintained that of the classified and highly classified networks. DoC investments also improved decision-makers' understanding of threats and vulnerabilities and better prepared mission staff to respond to risks at mission. On the other hand, while critical to the overall safety and security of missions, persistent challenges in the planning and delivery of major and minor physical security projects, as well as security equipment and systems, limited the security and resilience of mission infrastructure and security posture. In addition, there was a lack of consistent GBA Plus considerations in DoC envelope planning and delivery which led to challenges given the diverse range of stakeholder groups at mission and the differential risks they faced.

Recommendations and considerations

Recommendations: 2017-2027 DoC envelope

Recommendations 1 through 4 aim to inform course corrections and improvements to the planning and delivery of the DoC envelope during the second half of its mandate (2024-25 to 2026-27).

1

Security risk assessment and mitigation [Primary support from Finding [15](#); secondary support from Findings [3](#), [6](#), [11](#), [13](#), [14](#), and [16](#)]¹³

CFM, in partnership with ACM, HCM, IFM, SCM, and in consultation with missions, should improve risk assessment models, methodologies, processes, systems and tools to effectively capture and assess the growing complexity of threats and vulnerabilities experienced across the mission network and across diverse groups (such as women, 2SLGBTQI+, people with disabilities, racialized and indigenous peoples), translate them into well-scoped, prioritized mitigation measures and identify the potential impact of residual risk.

3

Major projects, minor projects and security equipment and systems [Primary support from Findings [4](#) and [9](#); secondary support from Findings [14](#), [15](#), [17](#), [18](#), and [19](#)]

ACM should monitor the impact of the recent structural, system and process changes made to improve the planning, implementation and tracking of DoC projects and take further course-corrections to address remaining challenges (including along the procurement/supply chain continuum), ensure timely project delivery (in particular for service line projects), meet DoC envelope commitments, and improve communication with other relevant branches and missions.

2

Decision-making and oversight [Primary support from Findings [15](#) and [16](#); secondary support from Finding [13](#)]

Building on the changes to SIPAB's leadership, mandate and composition, CFM should strengthen the governance structure under the Global Security Framework to ensure effective prioritization and allocation of the DoC envelope's resources in the remaining years of its mandate and to provide greater oversight of investments in high-risk and critical-risk missions.

4

Mission readiness teams [Primary support from Findings [8](#) and [12](#); secondary support from Finding [7](#)]

CFM, in consultation with HCM and missions, should develop a long-term strategy for the evolution of the mission readiness program, including for mission readiness team composition, training and staff assignments, to ensure appropriate alignment with mission safety and security needs, existing mission readiness team capacity and in consideration of available resources as well as apply a GBA Plus lens. The strategy should ensure a balance between security and operational priorities to support inclusive and effective international cooperation while maintaining an appropriate standard of care.

¹³ See Annex XII for a detailed breakdown of the evaluation line of evidence in support of the recommendations.

Recommendations: Forward-looking (beyond 2027)

Recommendations 5 and 6 are forward-looking and aim to support the planning and design of the next iteration of departmental mission security investments and programming beyond the 2016 DoC MC timeframe (2017-18 to 2026-27).

5

Clarity of safety and security responsibilities and accountabilities [Primary support from Finding [14](#); secondary support from Findings [13](#), [15](#) and [16](#)]

CFM, in consultation with ACM, HCM, IFM, SCM, geographic branches and USS, should leverage and build upon existing relevant frameworks to develop a comprehensive departmental security policy and guidance that articulates up-to-date authorities, responsibilities and accountabilities of organizational units, departmental officials and governing bodies involved in safety and security investments and programming at Canada's missions abroad, including accountabilities for accepting unmitigated or residual risk.

6

Scope of GAC's duty of care responsibilities and resourcing strategy [Primary support from Findings [1](#), [2](#) and [3](#); secondary support from Findings [11](#), [18](#) and [20](#)]

To inform planning for the next iteration of departmental mission security investments and programming beyond the 2016 DoC MC timeframe (2017-18 to 2026-27):

- CFM, in partnership with ACM, HCM, IFM, JFM, SCM and geographic branches, should define, document, and communicate the full scope of departmental responsibilities to protect people, information and assets at missions abroad, taking into consideration the needs of diverse stakeholder groups, including but not limited to women, 2SLGBTQI+, people with disabilities, racialized and indigenous peoples and mission security contexts.
- CFM, in partnership with ACM, HCM, IFM and SCM, should develop resourcing strategies to implement effective and sustainable solutions to protect infrastructure, information and people abroad, based on an assessment of the gaps in GAC's ability to meet its responsibilities and the capacity of departmental teams to implement solutions.

Considerations for Global Affairs Canada

Linkages to the Transformation Implementation Plan *[Primary support from Findings [1](#), [2](#), [3](#); secondary support from Findings [11](#) and [18](#)]*

GAC has embarked on an ambitious, multi-year Transformation Implementation Plan (TIP) to transform its operations to better deliver on departmental mandates and meet the challenges of the future. Several pillars of the TIP include action items and outcomes with implications for GAC's safety and security investments, particularly in times of crisis. As part of this exercise, the department should proactively and clearly identify how the department's safety and security investments can be considered in the implementation of the TIP.

GAC's legal duty of care responsibilities for LES and contractors *[Primary support from Finding [11](#); secondary support from Finding [3](#)]*

Evaluation evidence pointed to a lack of awareness among stakeholders of the department's specific legal DoC responsibilities in relation to LES and contractors working at missions abroad, and particularly in times of crisis. This could result in a gap between what LES and contractors expect and the actual standard of care provided. GAC (both HQ and missions) would benefit from clarifying its legal DoC responsibilities, in particular the appropriate standard of care, and transparently communicating this to these stakeholder groups.

Whole-of-government collaboration *[Primary support from Findings [1](#), [2](#), [3](#) and [20](#)]*

GAC relies on federal partners in their role as common services providers or subject matter experts to deliver its safety and security initiatives, including those funded by the DoC envelope. The scope of interdepartmental collaboration and relationships with federal partners have fluctuated over the evaluation period, resulting in gaps in service and increased financial and human resource pressures on the department. Reviewing the nature, scope and processes for whole-of-government collaboration and aligning cross-departmental priorities would improve the delivery of more sustainable safety and security initiatives.

Capacity of GAC's professional security cadre *[Primary support from Findings [8](#) and [18](#)]*

GAC has made investments to professionalize security resources at HQ and at missions; however, gaps remained in the depth of security expertise and the availability of skilled practitioners to meet departmental needs. The evolving nature and complexity of security threats across the mission network, particularly those related to cybersecurity, espionage and advancements in artificial intelligence, continue to put pressure on the department's security resources to keep pace. To ensure that GAC maintains its ability to mitigate current and future threats, it should consider strategies to bolster the capacity of its professional security cadre (both at HQ and mission), including by tapping into security expertise from other federal departments and the private sector.

Annexes

Annex I: Evaluation of Mission Security and Personal Safety Abroad (2016)

Recommendations from the 2016 evaluation

Recommendation #1: The department should design a global security framework to address security risks at its missions abroad. The framework should be based on timely and relevant threat and vulnerability assessments that are then analyzed against sets of security standards to determine both physical and operational enhancements at our missions abroad.

Recommendation #2: The department should streamline its governance structure for mission security and better define accountabilities, roles and responsibilities for departmental officials.

Recommendation #3: The department should continue with the professionalization of the security program and consider expanding SPM/MPSS coverage, roles and responsibilities.

Recommendation #4: The department should embrace a security culture at all levels and ensure that there is a shared responsibility for security that enables successful program delivery at missions abroad.

In 2016, GAC conducted an evaluation of Mission Security and Personal Safety Abroad to provide the department's senior management with a neutral and evidence-based assessment of the relevance and performance of mission security initiatives. **The evaluation produced a number of key findings:**

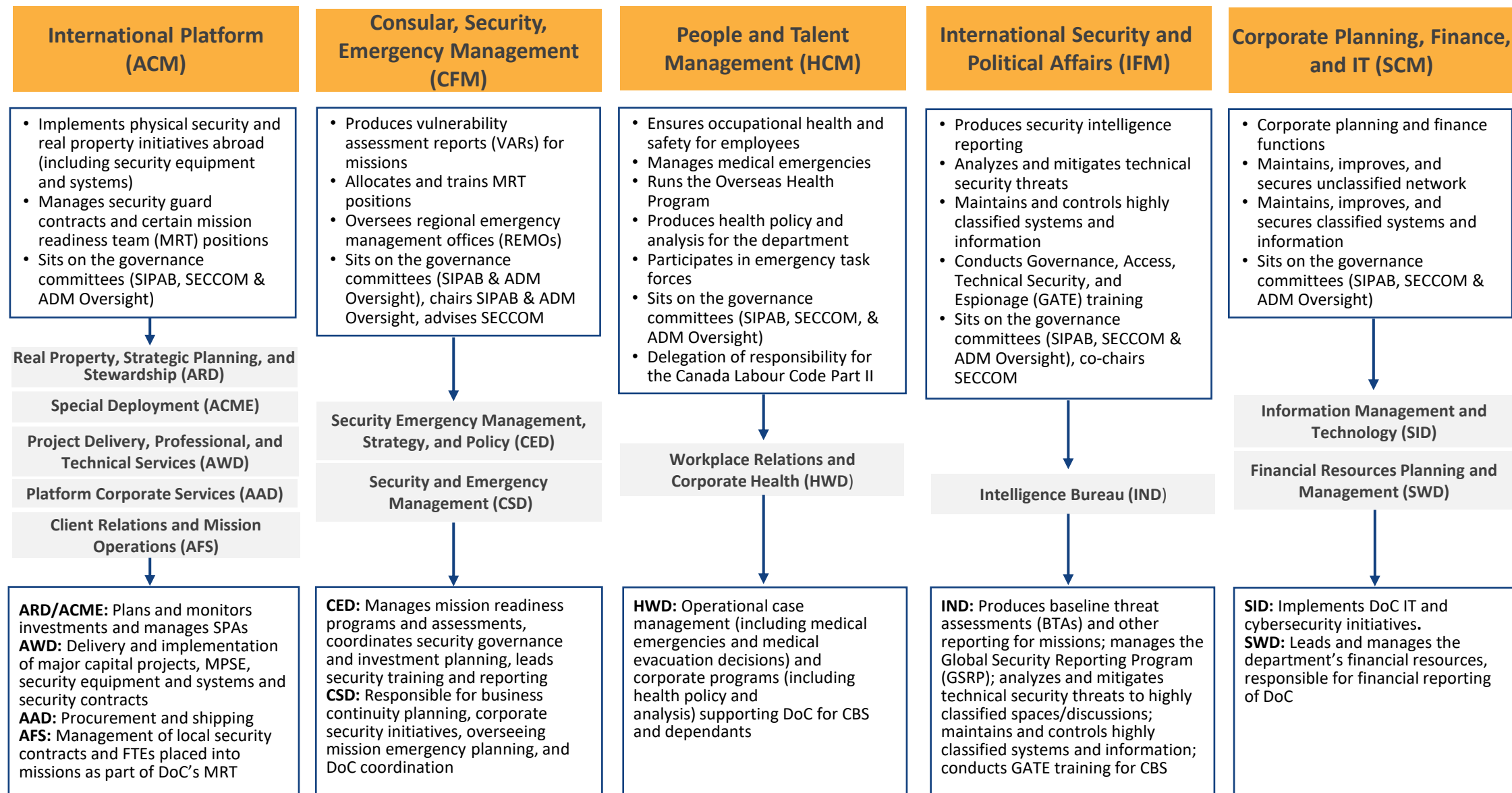
- ❖ The nature of threats to Canadian missions and personnel abroad changed substantially over the years and continued to evolve during the evaluation period. This changing global context, combined with Canada's evolving foreign policy and growing international presence, resulted in increased risks for missions.
- ❖ Canada's investments in mission security were significant in the years prior to the evaluation and, despite some delays, resulted in substantial improvements in mission security. However, the country's efforts were modest compared to some of our allies and fell short of comprehensively addressing the wide range of threats faced by Canada's diplomatic missions. The completion and implementation of physical security standards for missions abroad was recognized as a central component of assessing the security needs associated with the country's global presence and fulfilling GACs duty of care obligations.
- ❖ One of the greatest threats facing Canadian missions abroad was staff complacency regarding security measures and directives. A weak security culture at GAC, and low staff awareness of security processes reduced the effectiveness of security investments and increased the department's vulnerabilities. There was a lack of consistency in staff training, awareness and due diligence regarding security procedures and protocols.
- ❖ The Security Program Manager (SPM) and Military Police Protective Services (MPSS) programs were especially effective in increasing security capacity and expertise at missions abroad. Missions with a dedicated SPM/MPSS had a stronger security culture, a greater ability to identify and mitigate security threats, and a greater capacity to respond to security incidents and situations.
- ❖ The mission security governance structure evolved in the years covered by the evaluation to include a greater number of stakeholders in the decision-making process. While this increased the flow of information regarding mission security, it also blurred roles and responsibilities and reduced accountability for mission security and personal safety abroad. There was a need to streamline the mission security governance structure to improve decision-making and establish clear accountabilities.

Annex II: List of DoC envelope financial instruments

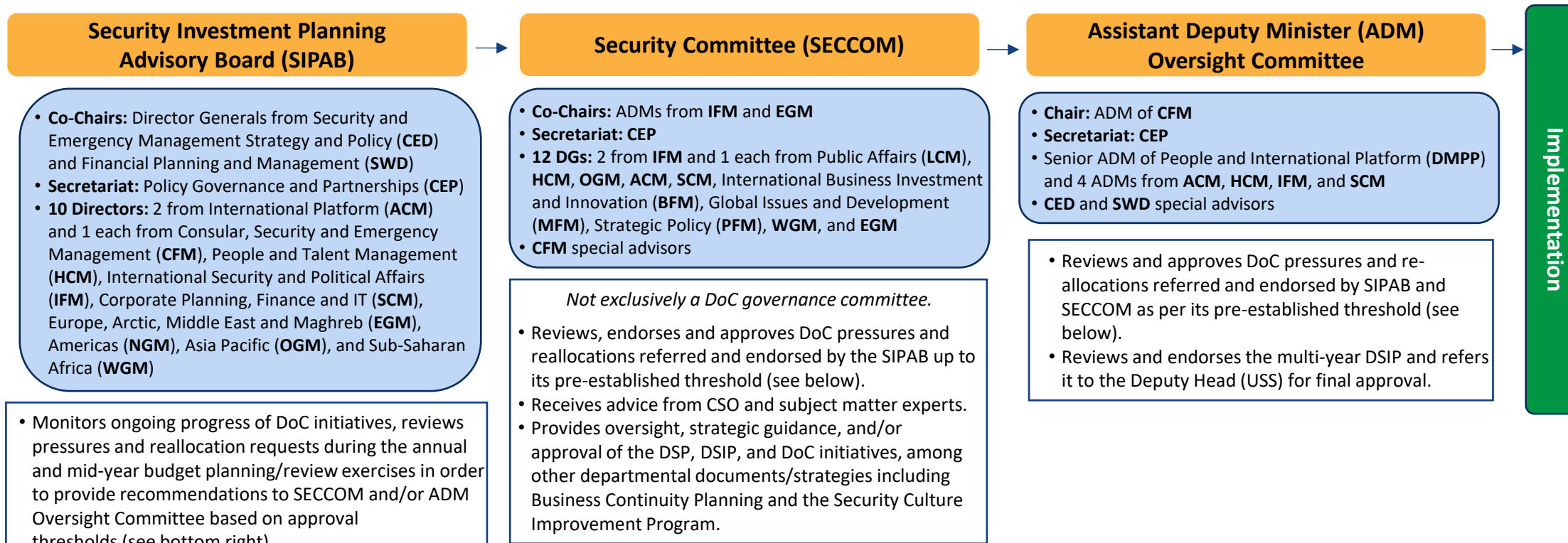
Title	Amount*	Details
2017 Duty of Care TB Submission	\$1.18B	In October 2017, Treasury Board (TB) approved GAC's duty of care submission to access most of the funding, including funding for operations and the security guard services contract in KABUL, for a total of \$1.18B over 10 years and \$105M ongoing.
2019 Colombo Chancery Relocation TB submission	\$5.7M	April 2019
2021 KABUL Mission Security and Operations 2021-24 TB submission (based on 2020 MC on Canada's Renewed Engagement Strategy in Afghanistan)	\$66M	This TB submission sought to advance contracting approval for a security guard contract and access to incremental funding of \$66M, not included in the \$1.87B, for the contract and mission operating costs for 3 additional years.
2021 Real Property Authorities for Missions Abroad TB submission	\$25M	This TB submission sought the transfer of 6 project approval authorities from a 2015 TB-approved Mission Security Infrastructure Submission under GAC's Organizational Project Management Capacity Assessment (OPMCA) authorities. The submission also sought full expenditure authority for the Colombo chancery relocation project and access to the related funding from the duty of care allocation in the fiscal framework to complete the construction of the chancery.
2021 Duty of Care TB submission	\$440M	This TB submission provided GAC with an additional \$440M over 6 years and \$8.4M in annual ongoing funding to implement the bulk of the remainder of the duty of care activities from 2021-22 to 2026-27. The funding was sought through Supplementary Estimates with the remainder to be allocated in Main Estimates.

*As of March 2022, there is a balance of \$232M and \$13.4M ongoing remaining in the fiscal framework in Vote 5.

Annex III: Key branches and bureaus involved in DoC planning and delivery



Annex IV: DoC governance committees



- Monitors ongoing progress of DoC initiatives, reviews pressures and reallocation requests during the annual and mid-year budget planning/review exercises in order to provide recommendations to SECCOM and/or ADM Oversight Committee based on approval thresholds (see bottom right).
- Integrates and prioritizes investments between/across DoC funding streams and provides advice to SECCOM on security-related funding requests.
- Receives advice from the Chief Security Officer (CSO) and subject matter experts.
- Coordinates security, geographic and functional subject matter expert review and input into DSIP.
- Submits security investment plans and recommends in-year adjustments to the SECCOM.

Pressures and Reallocations Approval Thresholds

	Vote 1		Vote 5	
	In Year	Multi-year/Ongoing	In Year	Multi-year/Ongoing
<500k	New: SIPAB Reallocation: Impacted bureau(s) DGs	SECCOM	New: SIPAB Reallocation: Impacted bureau(s) DGs	SECCOM
500k - \$2M	SIPAB		SIPAB	
\$2M - \$5M	SECCOM			
\$5M - \$10M	SECCOM			
>\$10M	ADM DoC Oversight Committee			

Annex V: Abridged evaluation matrix

Evaluation issue	Evaluation question	Evaluation sub-questions	Lines of evidence
Relevance and responsiveness	1.0 To what extent was the DoC envelope relevant and responsive to the needs and priorities of key stakeholders?	1.1 To what extent was the DoC envelope aligned with GAC's mandate, policies and priorities?	Document review HQ key informant interviews (HQ KIIs) Environmental scan Financial analysis
		1.2 To what extent was the DoC envelope and its funded initiatives aligned to the safety and security needs of key stakeholders?	Document review HQ KIIs Mission survey Mission case studies Environmental scan
		1.3 To what extent was the DoC envelope and its funded initiatives responsive to the evolving needs of key stakeholders?	Document review HQ KIIs Mission survey Mission case studies Financial analysis
		1.4 To what extent were DoC-funded initiatives aligned with the original pillars of the 2017 Treasury Board submission?	Document review HQ KIIs Mission survey Mission case studies
Effectiveness (results)	2.0 What progress has the DoC envelope made to achieving its objectives and results to date?	2.1 What results were obtained through DoC funding (positive, negative, intended, unintended) so far? <i>Note: 2.1 Also covered 2.3 from the evaluation design: "To what extent did the DoC envelope make initial progress towards its intended purpose as per the 2017 TB submission"?</i>	Document review HQ KIIs Mission survey Mission case studies
		2.2 To what extent did different groups (e.g., CBS, LES, Women, Children, 2SLGBTQI+) experience DoC results differently? Why?	Document review HQ KIIs Mission survey Mission case studies
		2.3 What factors affected (positively or negatively) progress towards results (e.g. COVID-19 pandemic)?	Document Review HQ KIIs Mission survey Mission case studies

Annex V: Abridged evaluation matrix (cont'd)

Evaluation issue	Evaluation questions	Evaluation sub-questions	Lines of evidence
Efficiency	3.0 To what extent did the DoC envelope structures, systems and processes* enable and/or hinder it to deliver on its mandate?	<p>3.1 To what extent did the DoC structures, systems and processes enable and/or hinder DoC program delivery, including:</p> <ul style="list-style-type: none"> flexible and responsive funding/programming based on evolving needs? timely allocation of funding to address needs? <p><i>Note: 3.1 Also covered 3.2 from the evaluation design: "To what extent did the DoC structures, systems and processes enable and/or hinder timely allocation of funding to address needs?"</i></p>	Document review HQ KIIs Mission survey Mission case studies Financial analysis Environmental scan
		<p>3.2 To what extent did the DoC structures, systems and processes enable and/or hinder an accurate prioritization of funding and programming?</p>	Document review HQ KIIs Mission survey Mission case studies Financial analysis Environmental scan
		<p>3.3 To what extent did the DoC structures, systems and processes enable and/or hinder its ability to define, track, measure, and report on results?</p>	Document review HQ KIIs Mission survey Mission case studies
Coherence**	4.0 To what extent was the DoC envelope implemented in a coherent manner?	<p>4.1. To what extent were there coordination and cooperation between the departmental units responsible for operationalizing the DoC envelope?</p>	Document review HQ KIIs Mission survey Mission case studies Environmental scan
		<p>4.2. How were the DoC envelope definition and purpose understood among different DoC actors within the department?</p>	Document review HQ KIIs Mission case studies Environmental scan

*Examples of structures, systems and processes include but are not limited: DoC governance structures and processes, DoC business processes, IM/IT systems and processes, organizational structures (division of responsibilities).

**Coherence in the context of the evaluation includes:

- interactions, synergies, coordination, duplications/gaps between the different DoC pillars, the departmental units responsible for them, and their programming priorities and objectives.
- understanding(s) of the DoC envelope's definition and purpose among different DoC actors within the department.

Annex VI: DoC evaluation methodology

Mixed methods (MM) with intention

MM was applied both **in parallel and sequentially** throughout the data collection phase of the evaluation.

- ❑ **Parallel MM** entailed conducting 2 or more methods at the same time. Each method complemented the other, allowing the evaluation team to triangulate data across multiple sources and methods in real time. This added explanatory value, strengthened the validity of data and enriched data analysis in the development of findings, conclusions and recommendations.
- ❑ **Sequential MM** was employed strategically, where one method followed the other with intention. While this also supported triangulation and the complementarity of data, the goal was for preceding methods to inform the development of subsequent methods. Subsequent methods also helped confirm and explain data already analyzed.

The evaluation data collection and analysis process used parallel and sequential mixed methods (see sidebar) as per the 5 phases described below:

Phase 1 (Jan. 2023 to March 2023): Document review, financial analysis, environmental scan and case study design

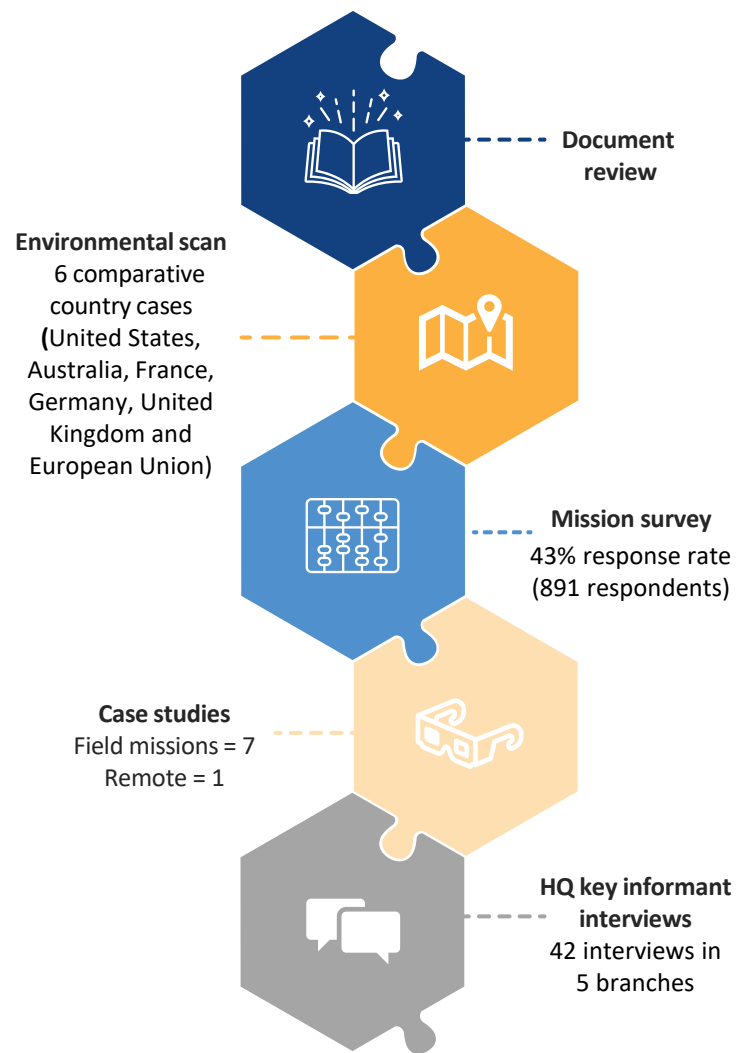
Phase 1 of the evaluation focused on desk-based research. The evaluation team conducted a financial analysis exercise and reviewed key DoC envelope documentation (including annual reports to Treasury Board and foundational DoC frameworks, planning and tracking tools). This provided the team with initial secondary data against the 4 evaluation questions as well as background knowledge on the DoC envelope's design, budget, governance structure, business process and results. This initial desk-based research informed the development of the online mission survey and the first draft of the case study design, including the sampling design and selection of cases (missions). In total 8 missions were selected as case studies (7 field missions and 1 remote). The desk review also informed the design for the environmental scan of Canada's security partners and their comparable DoC policies, approaches and programming.

Phase 2 (April 2023 to June 2023): Case studies and mission survey launch

Phase 2 focused on conducting field mission case studies and launching the mission survey. The 7 field mission case studies entailed supplemental document review (specific to each case), key informant interviews (KIIs) with DoC decision-makers/implementers (and in some cases, beneficiaries), focus group discussions (FGD) with DoC beneficiaries (CBS, their dependants and LES) as well as direct observation. FGDs allowed participants to explore and discuss key issues related to DoC, with the evaluation team acting as a facilitator to guide the discussion. KIIs and FGDs for field mission case studies took place in-person wherever possible. Where circumstances did not allow, they were done remotely. Data collection for the KABUL case study was done remotely, using available technology and did not include FGDs or direct observation. The value-added of field mission-based case studies was the ability for the evaluation team to situate themselves at Canadian missions in real time, where direct observations on DoC were experienced and noted. These opportunities allowed the team to dig deeper into the complexity of operating in various dynamic global security environments and generated a more in-depth understanding of DoC envelope delivery and the challenges that arose in specific contexts and on specific themes/issues. The selection of missions for in-person data collection was based on a structured methodology with the primary focus on learning. However, feasibility (e.g. security, COVID-19, logistics) was also considered in the final selection of cases. In May 2023, the mission survey was launched for 2 DoC stakeholder groups at mission (decision-makers/implementers and mission staff [CBS/LES]) to collect quantitative data against all 4 evaluation questions from the unique perspectives of those in the field.

Annex VI: DoC evaluation methodology (cont'd)

DoC evaluation data collection methods



Phase 3 (June 2023 to Sept. 2023): HQ key informant interviews (KIIs) and mission survey data analysis

Informed by phases 1 and 2, in phase 3 the evaluation team designed semi-structured key informant interview (KII) guides and conducted 42 in-depth KIIs with representatives across the 5 branches at HQ involved in DoC planning, delivery and reporting. Interviews were done both remotely and in person. A selection of interviews was conducted at a classified level, following appropriate departmental protocols to maintain the security of information. In parallel, the team also conducted initial data analysis from the mission survey that the team was able to leverage throughout the HQ KII process.

Phase 4 (Sept. 2023 to Dec. 2023): Data analysis and preliminary findings

Phase 4 focused on data analysis, storyboarding and the development of preliminary findings. Data analysis techniques included both qualitative and quantitative methods such as content analysis, thematic coding, descriptive statistics and comparative analysis. The team leveraged data analysis tools such as Microsoft Excel and NVivo. Non-classified qualitative data was coded using NVivo software to identify recurrent themes and their relationships, while quantitative data was analyzed using descriptive statistics in Excel. Throughout data collection and analysis, the evaluation team used different types of triangulation such as data triangulation, methodological triangulation and investigator triangulation. Following initial data analysis, the team engaged in a series of storyboarding sessions where evidence was discussed and analyzed in detail within the evaluation team to further ensure the validity and reliability of the evaluation's preliminary findings. In parallel, the team completed 2 final case studies (1 in-person field mission; 1 remote).

Phase 5 (Jan. 2024 to April 2024): Stakeholder engagement and report writing

In phase 5, the evaluation team engaged with the 8 case study missions, the evaluation's 5 office of primary interest (OPI) focal points as well as the DoC ADM Oversight Committee to validate the preliminary findings and identify factual discrepancies and/or data gaps. The evaluation team then updated the preliminary findings, completed supplementary data analysis and drafted the DoC evaluation report for approval by the Performance Measurement and Evaluation Committee (PMEC) in May 2024.

Annex VII: DoC envelope theory of change*

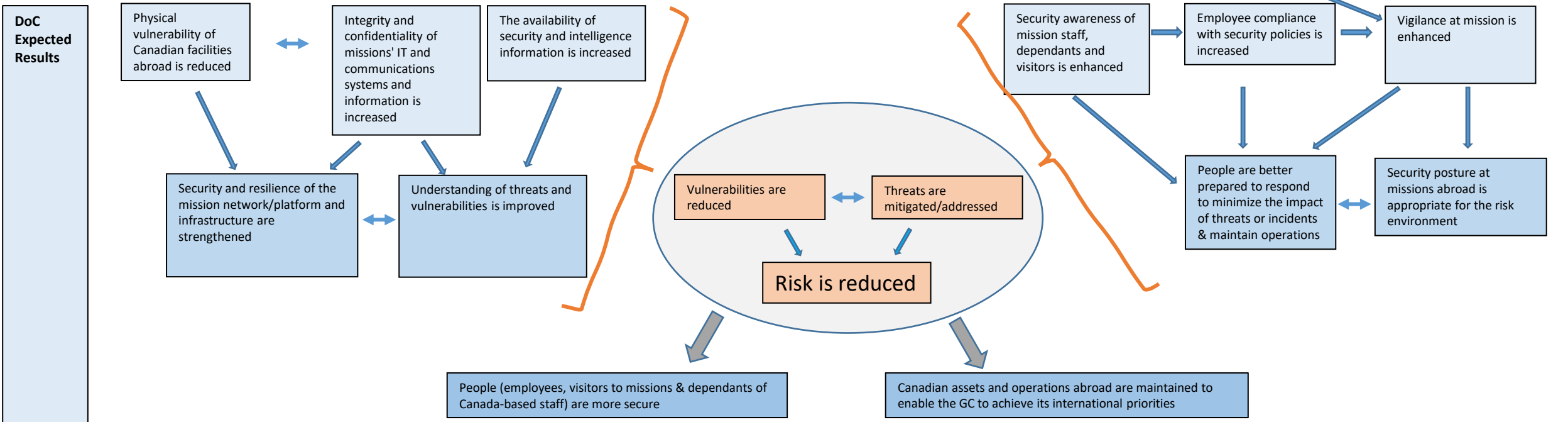
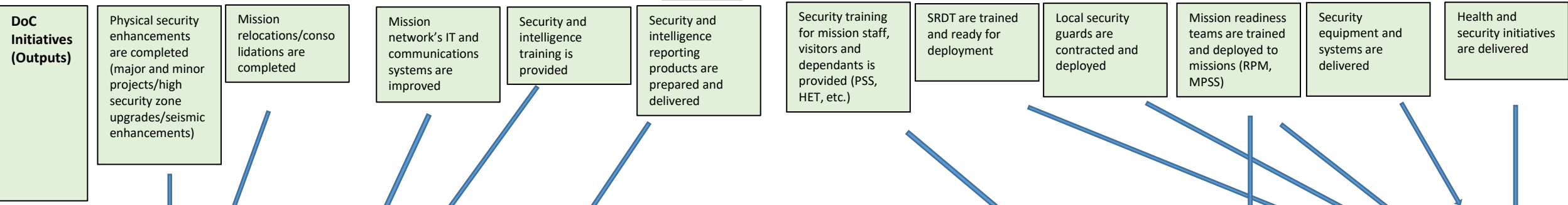
Inputs: DoC Envelope Funding, Human Resources

Internal Key Factors: Policies, frameworks, processes, systems, structures, division of responsibilities, etc. related to the DoC

Pillar 1**

Pillar 2

Pillar 3



*The ToC was informed by the Security Performance Measurement Framework (SPMF) in the DSIP, Annex A of the DSP (Logic Model) and the DSP implementation Matrix.

**Note For Pillar 4 Protecting our People in Kabul: Following the August 2021 evacuation of the Canadian Mission in Afghanistan, Pillar 4 initiatives have been suspended. Prior to the evacuation, investments in Kabul related to DoC were reflected in the results chain.

Annex VIII: DoC in times of crisis - Lessons from KABUL

The DoC envelope provided significant resources necessary to sustain Canada's diplomatic presence in Afghanistan until the suspension of mission operations in August 2021. The KABUL mission was both the costliest and one of the most dangerous in the GAC network. The mission dealt with complex and multi-faceted security risks that required self-sufficiency for security and emergency management in an increasingly hostile conflict environment. Risks were further exacerbated by the COVID-19 pandemic and the withdrawal of allied forces. Pillar 4 expenditures between 2017 and 2022 totalled \$84M.

Summary of lessons learned

The quality and continuity of **security guard services** are paramount in high-risk locations. Experience in KABUL highlighted the importance of focusing on best value rather than lowest contract cost and paying close attention to defining contract requirements to ensure quality service with adequate safeguards to mitigate risk. Elements to consider included: contractor guard selection; psychological and other supports (e.g. housing, transportation); investment in skill upkeep and practice; management of permits, visas and licences; evacuation plans and related costs; and guard remuneration. The change of service provider at the height of armed conflict added significant administrative workload, led to uncertainty and resulted in lower guard pay at the time of heightened threats.

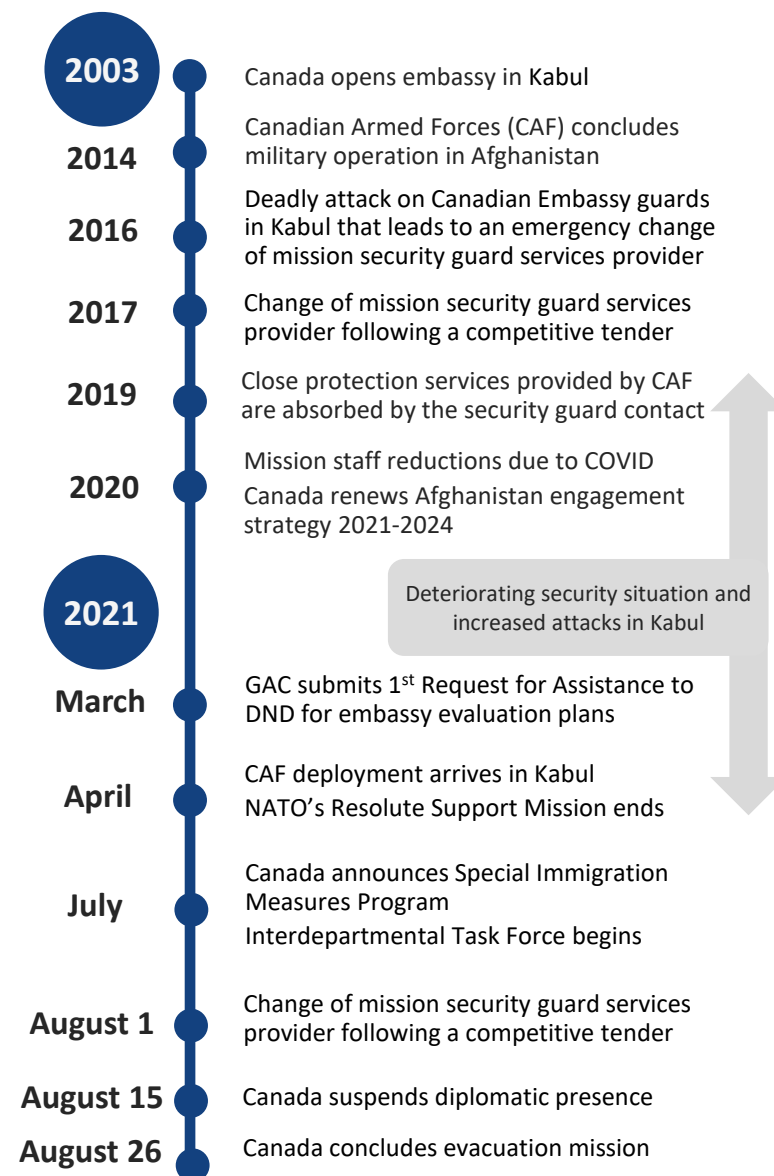
Investments in fortified **security infrastructure** (particularly bunkers, improvements to living quarters, perimeter security) reduced the physical vulnerability of the mission—in Kabul. However, the increased capabilities of insurgent groups, including rockets attacks, required continued timely investments and specialized delivery expertise.

Diplomatic operations in a conflict zone rely on **armoured vehicles, specialized equipment and personal protective equipment** in sufficient quantity, working order and durability. Procurement processes required greater flexibility than what was available due to a difficult operational context, with limited supplier availability, quality issues with available suppliers, and extreme pressures for timely delivery. Delays in accessing required equipment and the poor fit of some personal protective equipment, particularly for women, placed staff at risk.

On-the-ground intelligence to support mission operations in a rapidly evolving context was insufficient in the case of contracted resources in KABUL due to their limited ability to liaise with allies and access key intelligence sources. The introduction of Government of Canada intelligence capabilities in the field through GAC and Canadian Armed Forces resources in the last year of mission operations significantly improved strategic and emergency decision-making.

Mission **IT support** through skilled resources and continuous IT professional presence in the field through temporary duty assured mission access to classified communications.

Timeline of Events



Annex VIII: DoC in times of crisis - Lessons from KABUL (cont'd).

The **HOMs'** commitment to security, support for the mission readiness team and staff, knowledge of GAC's security landscape and surge options were critical to continued operation of the mission.

Successful **engagement and collaboration with the Canadian Armed Forces (CAF)** supported mission evacuation planning and execution and provided important intelligence and medical capabilities at a critical time. A consideration for a more active engagement and presence of CAF in support of diplomatic security in conflict locations were raised by interviewed staff.

The size, composition and capacity of the **mission readiness team** was not aligned with the threat environment in KABUL. The 24/7 nature of the security work, its volume, the compound set-up and the coordination with HQ and allies resulted in a heavy workload – without dedicated administrative support – for the readiness team. Many of the team's resources were new to security positions, while operating in complex, militarized zones would have strongly benefited from the deployment of the most experienced cadre with a background in risk assessment, the ability to coordinate with defence forces and the ability to effectively engage and communicate with staff. Optimizing the role of the military police to account for the role of contracted security services and the need for an internal mission defence capability with combat experience was cited by interviewees as a consideration.

The mission, with support from HQ, established and reviewed detailed **procedures and plans** to enable mission operations and emergency management. There was room to improve the clarity and testing of standard operating procedures in high-risk contexts, including preparation for worst-case scenarios.

Staff's preparedness for deployment and awareness of security risks was achieved through personal research and HET and was further strengthened through rigorous and extensive training and drills at the mission.

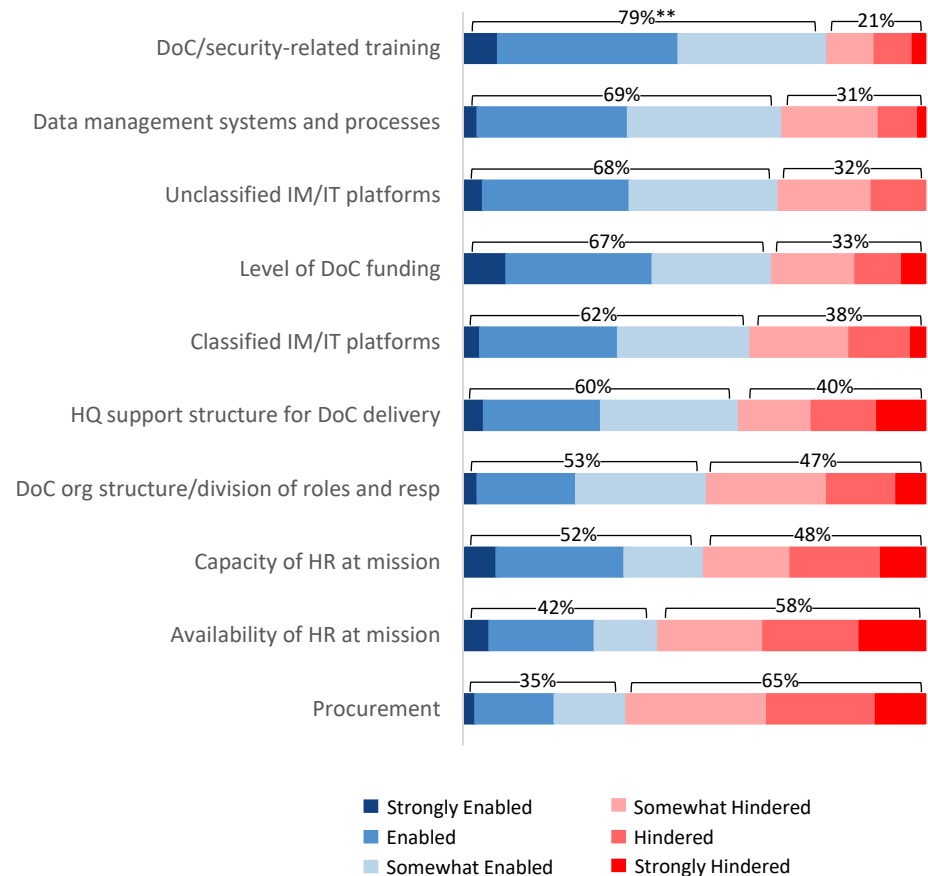
Experience in KABUL revealed that GAC employee support across the deployment-reintegration continuum had notable gaps. Identified **pre-deployment gaps** included a need for psychological, medical and suitability assessments, training on stress management and conflict resolution in the context of compound living. **Support during deployment** (such as rest and relaxation travel, Employee Assistance Program visits) was largely scaled down during the COVID-19 pandemic, while medical support was inadequate in relation to health threats and the mission context. As a result of these limitations, staff experienced significant negative impacts on their physical health, mental health and well-being that were not addressed post-deployment. LES and contracted guards also experienced significant negative outcomes. Staff's experience in KABUL underscored the importance of instituting targeted **reintegration support and recognizing** the efforts of staff who lived and worked under extreme conditions.

DoC for LES and contractors in KABUL

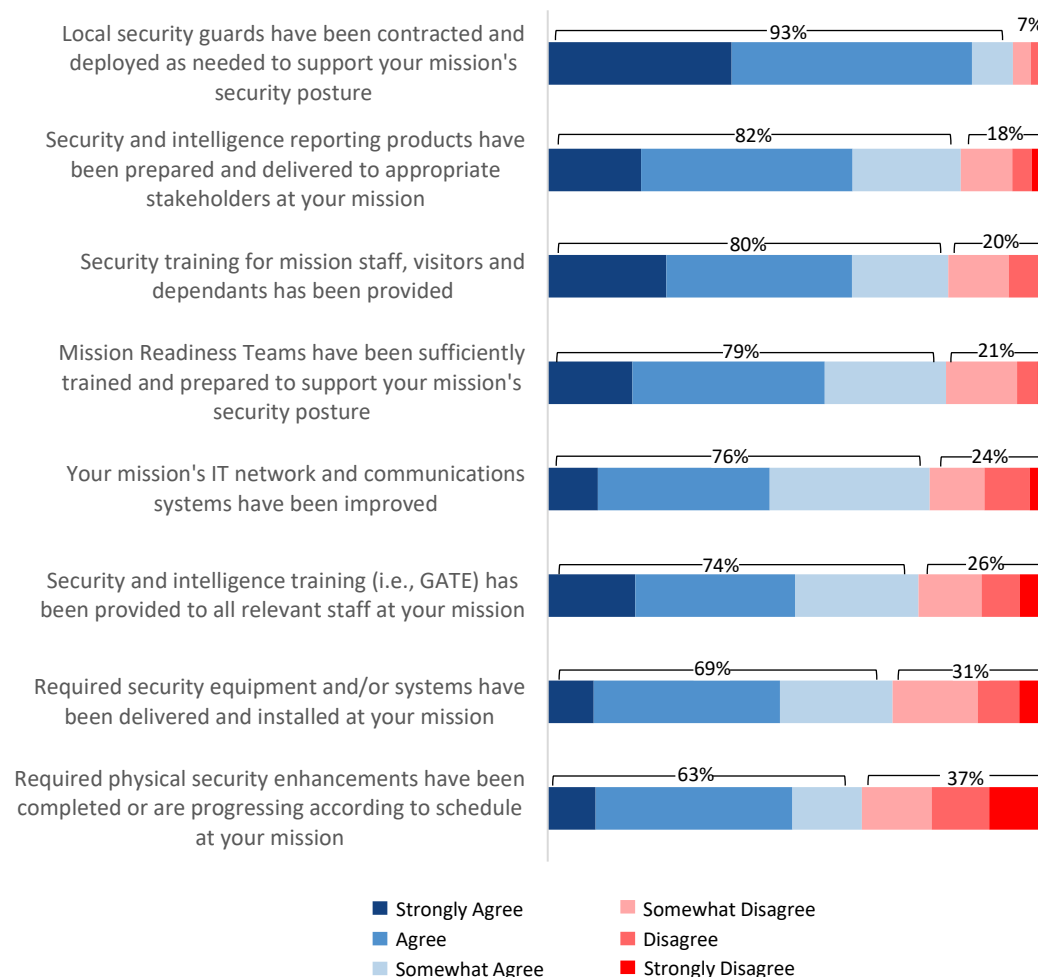
Experience in KABUL raised the issue of the Government of Canada's duty of care responsibility in relation to locally engaged staff and contracted resources, given their level of exposure to threats and in view of the conditions of the compound living (e.g. medical coverage and vaccination requirements, access to psychological support services, living arrangements, evacuation support). Canada evacuated locally engaged staff and their families.

Annex IX: Mission survey analysis – Delivery of DoC initiatives

Graph 1: Internal factors that hindered or enabled the delivery of safety and security initiatives according to DoC decision-makers and implementers*



Graph 2: DoC decision-makers and implementers' level of agreement with the delivery of DoC initiatives***



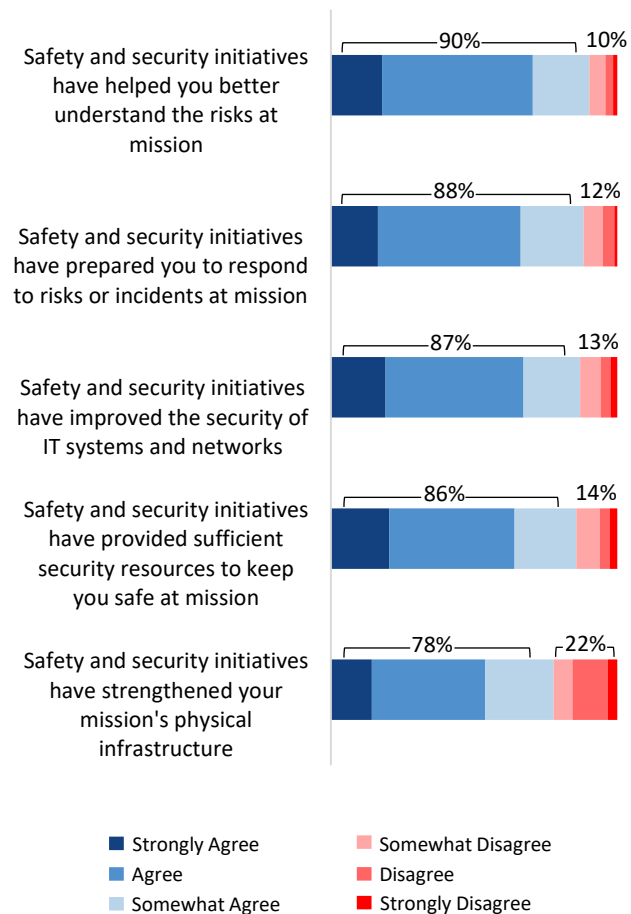
*Only decision-makers and implementers were asked the questions corresponding to graphs 1 and 2.

**displayed percentages represent aggregated survey results across the 6 categories (“at least somewhat enabled/agreed” and “at least somewhat hindered/disagreed”).

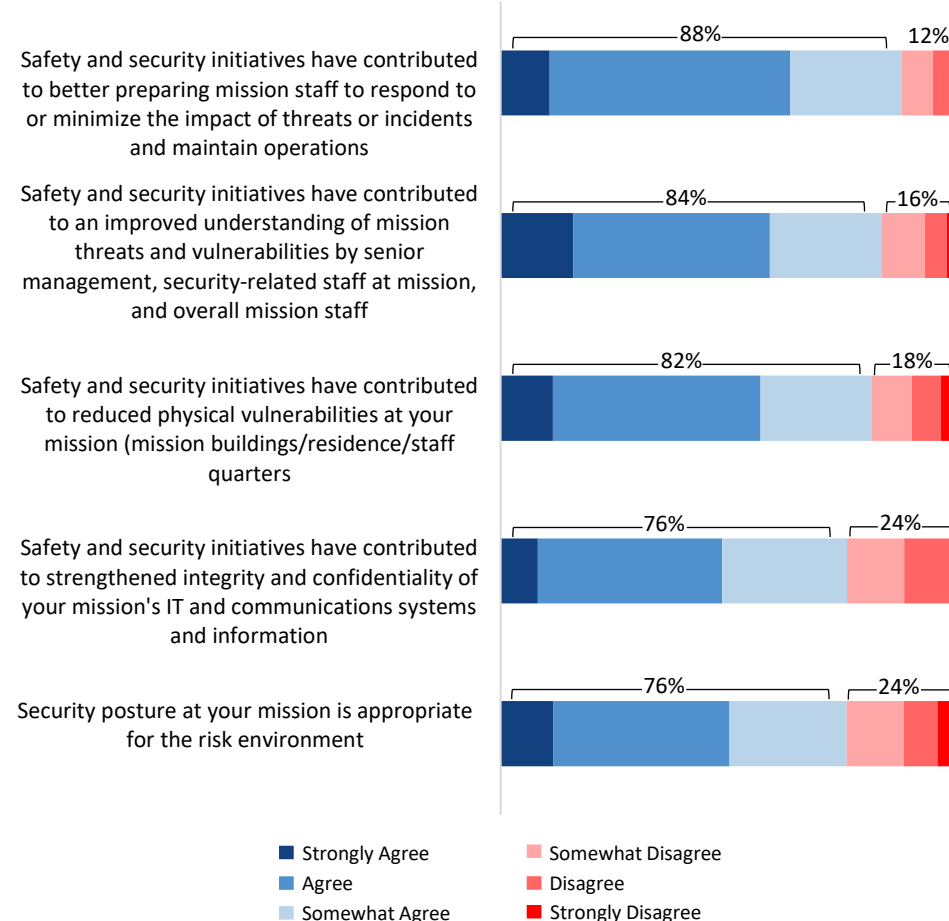
***excludes initiatives that were not commonly experienced across the mission network, including Standing Rapid Deployment Teams (SRDTs) and relocation/consolidation projects.

Annex IX: Mission survey analysis – Achievement of DoC results

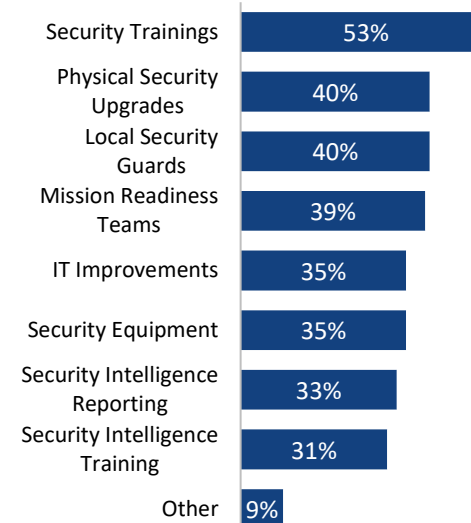
Graph 3: DoC beneficiaries' level of agreement with the achievement of DoC results



Graph 4: DoC decision-makers and implementers' level of agreement with the achievement of DoC results

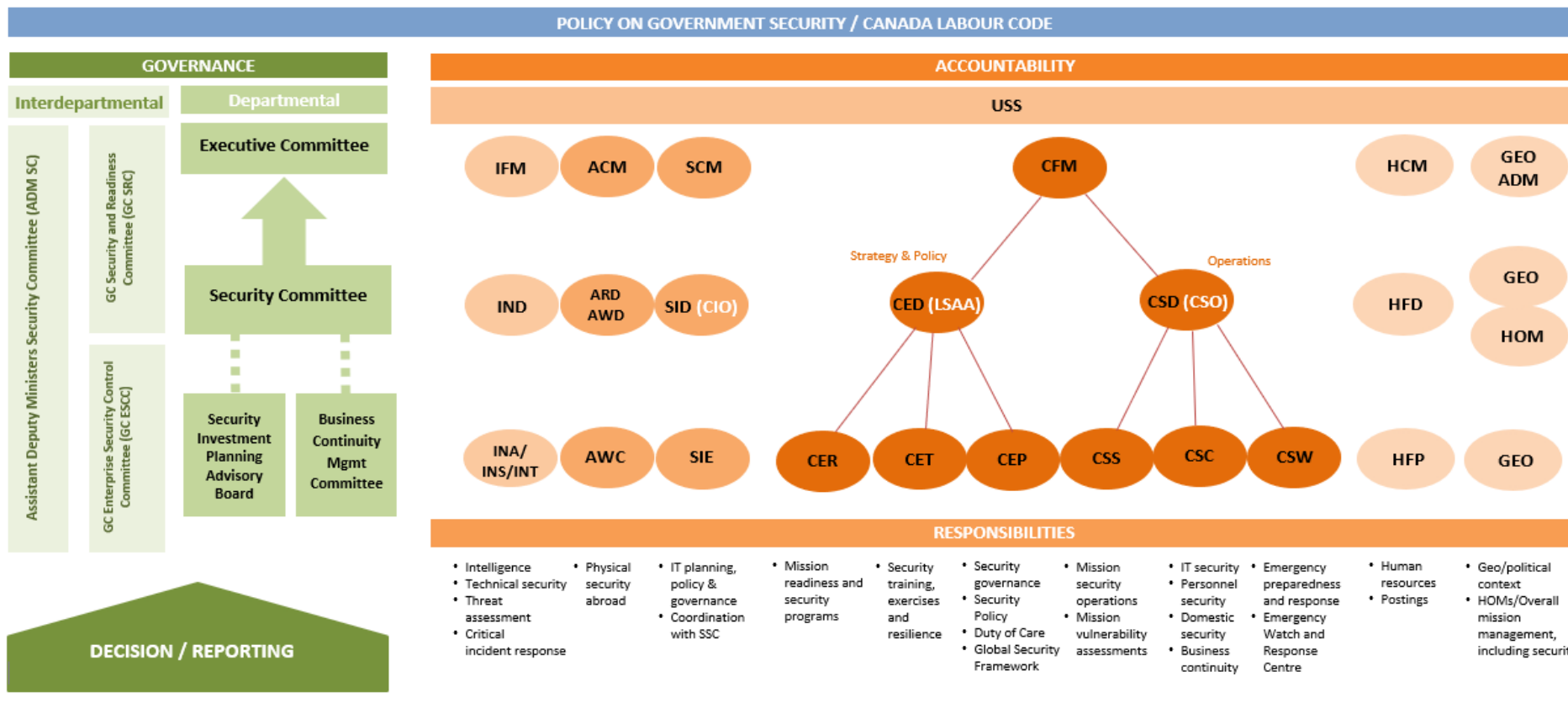


Graph 5: The most effective safety and security initiatives in terms of mitigating risks at mission according to DoC decision-makers and implementers



Annex X: Security Management and Governance Framework (SMGF)

Under the GSF, the **Security Management and Governance Framework (SMGF)** was designed to provide a high-level overview of the department's security structure, responsibilities, accountabilities and governance in Canada and missions abroad. The SMGF included, but was not limited to, the DoC envelope as it covered all departmental security, including domestic security (source: 2019-20 DSP, Annex B).



ACM = International Platform Branch
 ARD = Strategic Planning and Stewardship
 AWC = Physical Security Abroad
 AWD = Delivery, Professional & Technical Services
 CED = Security & EM (Strategy and Policy)
 CEP = Policy, Governance and Partnerships

CER = Mission Readiness & Security Programs
 CET = Planning, Training & Exercises
 CFM = Consular, Security and EM Branch
 CIO = Chief Information Officer
 CSC = Corporate Security
 CSD = Security & EM (Operations)

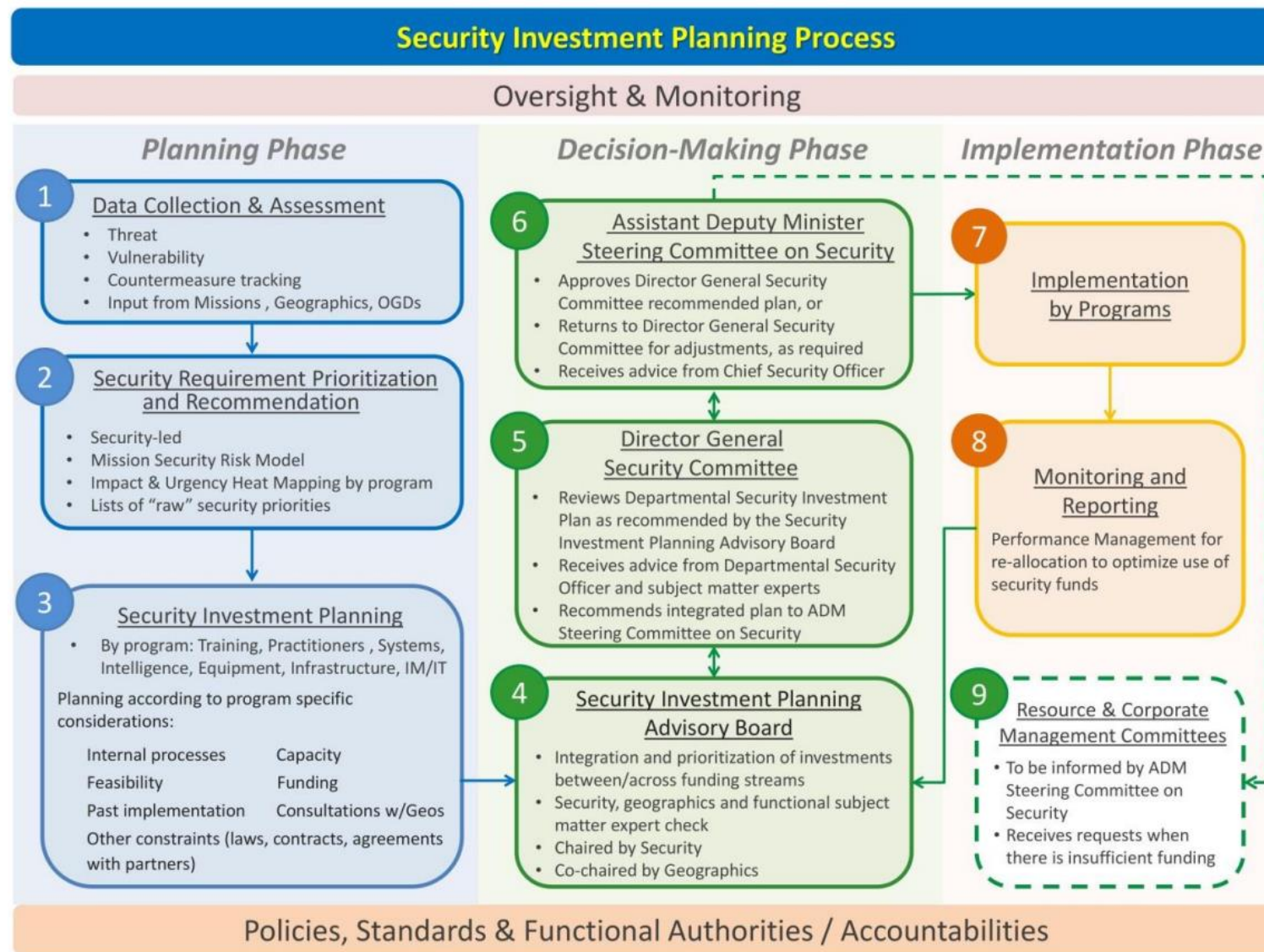
CSO = Chief Security Officer
 CSS = Mission Readiness & Security Operations
 CSW = Emergency Operations
 HCM = Human Resources Branch
 HFD = Assignments and Executive Management
 HFP = Assignment and Pool Management

IFM = Int'l Security & Political Affairs Branch
 INA = Intelligence Assessments & Reporting
 IND = Intelligence Bureau
 INP = Intelligence Policies and Programs
 INS = Intelligence Access & Counter-Measures
 INT = Threat Assessment

LSAA = Lead Security Agency Authority
 SCM = Corporate Planning, Finance & IT
 SID = Information Mgmt & Technology
 SIE = Client Relations & IT Governance
 USS = Deputy Minister of Foreign Affairs

Annex XI: Departmental Security Investment Plan (DSIP) process

The **DSIP process** was designed to integrate security investment planning across the department and was used to inform program-specific investment plans. The process involved 3 phases and a series of steps with the aim of allocating resources through a risk-based prioritization approach and by accounting for program-specific considerations (source: 2019-20 DSP).



Annex XII: Line of evidence from findings to recommendations

Recommendation	Primary support	Secondary support
<p>Recommendation 1: <i>Security risk assessment and mitigation</i></p> <p>CFM, in partnership with ACM, HCM, IFM, SCM, and in consultation with missions, should improve risk assessment models, methodologies, processes, systems and tools to effectively capture and assess the growing complexity of threats and vulnerabilities experienced across the mission network and across diverse groups (such as women, 2SLGBTQI+, people with disabilities, racialized and indigenous peoples), translate them into well-scoped, prioritized mitigation measures and identify the potential impact of residual risk.</p>	<p>Finding 15: The prioritization of DoC funding and programming was limited by the envelope’s complexity, the number and variety of stakeholders involved, competing priorities, and reliance on outdated systems, processes and tools.</p>	<p>Finding 3: Despite the envelope’s broad alignment to needs, there were additional safety and security priorities identified directly by key stakeholders and within departmental risk frameworks that were not part of the original DoC envelope design, notably in the area of health, safety and well-being.</p> <p>Finding 6: DoC investments improved decision-makers’ understanding of threats and vulnerabilities at mission through increased availability and diversity of security and intelligence information and new threat analysis capacities.</p> <p>Finding 11: While all demographics generally reported feeling safe or very safe at mission, the multiple stakeholder groups across the mission network experienced differences in the risks they faced.</p> <p>Finding 13: Specific structures, processes and mechanisms were leveraged and built into the envelope’s design to facilitate a responsive, risk-based approach to managing finite departmental security resources.</p> <p>Finding 14: The complex DoC delivery structure and the lack of a clear and comprehensive departmental security policy or directive resulted in blurred accountabilities, roles and responsibilities, and led to inefficiencies and challenges in coordination and collaboration.</p> <p>Finding 16: The DoC governance structure enabled a timely allocation of funding and was responsive to emerging needs and crises but did not sufficiently fulfill its challenge function.</p>
<p>Recommendation 2: <i>Decision-making and oversight</i></p> <p>Building on the changes to SIPAB’s leadership, mandate and composition, CFM should strengthen the governance structure under the Global Security Framework to ensure effective prioritization and allocation of the DoC envelope’s resources in the remaining years of its mandate and to provide greater oversight of investments in high-risk and critical-risk missions.</p>	<p>Finding 15: The prioritization of DoC funding and programming was limited by the envelope’s complexity, the number and variety of stakeholders involved, competing priorities, and reliance on outdated systems, processes and tools.</p> <p>Finding 16: The DoC governance structure enabled a timely allocation of funding and was responsive to emerging needs and crises but did not sufficiently fulfill its challenge function.</p>	<p>Finding 13: Specific structures, processes and mechanisms were leveraged and built into the envelope’s design to facilitate a responsive, risk-based approach to managing finite departmental security resources.</p>

Annex XII: Line of evidence from findings to recommendations (cont'd)

Recommendation	Primary support	Secondary support
<p>Recommendation 3: <i>Major projects, minor projects and security equipment and systems</i></p> <p>ACM should monitor the impact of the recent structural, system and process changes made to improve the planning, implementation and tracking of DoC projects and take further course-corrections to address remaining challenges (including along the procurement/supply chain continuum), ensure timely project delivery (in particular for service line projects), meet DoC envelope commitments, and improve communication with other relevant branches and missions.</p>	<p>Finding 4: DoC investments in strengthening mission physical infrastructure were critical for improving the safety and security of people across the network. However, slow project delivery, due to both internal and external challenges, limited the department's ability to address physical vulnerabilities at missions. Recent efforts have been made to address inefficiencies and boost capacity to improve project delivery.</p> <p>Finding 9: Delays in equipment and systems delivery hindered missions' readiness and limited their overall security posture.</p>	<p>Finding 14: The complex DoC delivery structure and the lack of a clear and relevant departmental security policy or directive resulted in blurred accountabilities, roles and responsibilities and led to inefficiencies and challenges in coordination and collaboration.</p> <p>Finding 15: The prioritization of DoC funding and programming was limited by its complexity, the number and variety of stakeholders involved, competing priorities, and reliance on outdated systems, processes, and tools.</p> <p>Finding 17: Tracking and reporting on DoC progress and results were not adequately robust to support evidence-based decision-making.</p> <p>Finding 18: Multiple interrelated human resources challenges hindered the timeliness and responsiveness of the delivery of DoC initiatives.</p> <p>Finding 19: Procurement processes and gaps in capacity contributed to delays in the delivery of DoC equipment, services and projects.</p>
<p>Recommendation 4: <i>Mission readiness teams</i></p> <p>CFM, in consultation with HCM and missions, should develop a long-term strategy for the evolution of the mission readiness program, including for mission readiness team composition, training and staff assignments, to ensure appropriate alignment with mission safety and security needs, existing mission readiness team capacity and in consideration of available resources as well as apply a GBA Plus lens. The strategy should ensure a balance between security and operational priorities to support inclusive and effective international cooperation while maintaining an appropriate standard of care.</p>	<p>Finding 8: The Mission Readiness Program overall contributed to improving vigilance and strengthening the missions' security posture. However, the success of this initiative varied greatly from mission to mission.</p>	<p>Finding 7: DoC-funded initiatives that had a deliberate focus on preparedness improved the capacity of mission staff to respond to and minimize the impact of threats and incidents abroad. However, these efforts were inconsistent across the mission network and between different stakeholder groups, including women, LES and 2SLGBTQI+, among others.</p> <p>Finding 12: Security protocols could hinder staff's ability to deliver programming if they were overly restrictive and not sufficiently informed by evidence. Restrictions were generally welcomed in higher threat environments.</p>

Annex XII: Line of evidence from findings to recommendations (cont'd)

Recommendation	Primary support	Secondary support
<p>Recommendation 5: <i>Clarity of safety and security responsibilities and accountabilities</i></p> <p>CFM, in consultation with ACM, HCM, IFM, SCM, geographic branches and USS, should leverage and build upon existing relevant frameworks to develop a comprehensive departmental security policy and guidance that articulates up-to-date authorities, responsibilities and accountabilities of organizational units, departmental officials and governing bodies involved in safety and security investments and programming at Canada's missions abroad, including accountabilities for accepting unmitigated or residual risk.</p>	<p>Finding 14: The complex DoC delivery structure and the lack of a clear and comprehensive departmental security policy or directive resulted in blurred accountabilities, roles and responsibilities, and led to inefficiencies and challenges in coordination and collaboration.</p>	<p>Finding 13: Specific structures, processes and mechanisms were leveraged and built into the envelope's design to facilitate a responsive, risk-based approach to managing finite departmental security resources.</p> <p>Finding 15: The prioritization of DoC funding and programming was limited by the envelope's complexity, the number and variety of stakeholders involved, competing priorities, and reliance on outdated systems, processes and tools.</p> <p>Finding 16: The DoC governance structure enabled a timely allocation of funding and was responsive to emerging needs and crises but did not sufficiently fulfill its challenge function.</p>
<p>Recommendation 6: <i>Scope of GAC's duty of care responsibilities and resourcing strategy</i></p> <p>To inform planning for the next iteration of departmental mission security investments and programming beyond the 2016 DoC MC timeframe (2017-18 to 2026-27):</p> <ul style="list-style-type: none"> CFM, in partnership with ACM, HCM, IFM, JFM, SCM and geographic branches, should define, document, and communicate the full scope of departmental responsibilities to protect people, information and assets at missions abroad, taking into consideration the needs of diverse stakeholder groups, including but not limited to women, 2SLGBTQI+, people with disabilities, racialized and indigenous peoples and mission security contexts. CFM, in partnership with ACM, HCM, IFM and SCM, should develop resourcing strategies to implement effective and sustainable solutions to protect infrastructure, information and people abroad, based on an assessment of the gaps in GAC's ability to meet its responsibilities and the capacity of departmental teams to implement solutions. 	<p>Finding 1: The Duty of Care envelope built on the department's evolving approach to mission security and aligned with GAC's mandate to comprehensively manage cross-mission security needs in a dynamic global security environment.</p> <p>Finding 2: The DoC envelope and initiatives broadly aligned with the department's security priorities, and mostly addressed the safety and security needs identified by mission stakeholders.</p> <p>Finding 3: Despite the envelope's broad alignment to needs, there were additional safety and security priorities identified directly by key stakeholders and within departmental risk frameworks that were not part of the original DoC envelope design, notably in the area of health, safety and well-being.</p>	<p>Finding 11: While all demographics generally reported feeling safe or very safe at mission, the multiple stakeholder groups across the mission network experienced differences in the risks they faced.</p> <p>Finding 18: Multiple interrelated human resources challenges hindered the timeliness and responsiveness of the delivery of DoC initiatives.</p> <p>Finding 20: Divergent priorities and capacity limitations among federal partners to support the implementation of some DoC initiatives put pressure on envelope resources and led to gaps in GAC's ability to ensure the protection of staff, information and assets abroad.</p>