Treasury Board of Canada Secretariat | Secrétariat du Conseil du Trésor du Canada

Management Accountability Framework (MAF) Round VI

Security and Business Continuity Area of Management (AoM) #19

Training Session
October 2008

RDIMS #686129

Canada

Purpose

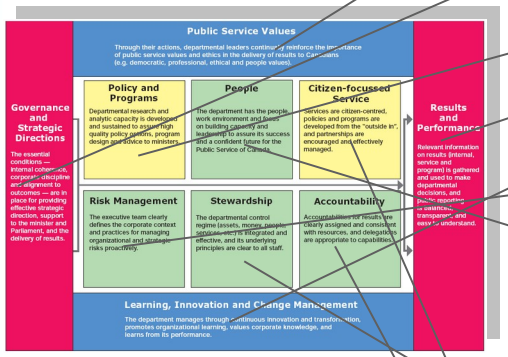
- Provide training to departmental staff responsible for preparing the MAF response for Area of Management (AoM) 19 (Security and Business Continuity)

- Training will cover the assessment methodology and evidence requirements for AoM 19, with a **special focus** on:
  - **New response template for AoM 19**
  - **Line of evidence 19.1 (Departmental Security Program)**

- Questions related to the other lines of evidence can be addressed at the end of the session

AoM 19 in MAF Assessment System

Expectations



***** New area of management in MAF V (MITS assessed with IT then IM in previous rounds)**

Security and Business Continuity (part of Stewardship element)

Areas of Management

1. Values and Ethics
2. Corporate Performance Framework
3. Corporate Management Structure
4. Extra-Organizational Contribution
5. Quality of Analysis
6. Evaluation
7. Performance Reporting to Parliament
8. Managing Organizational Change
9. Risk Management
10. Workplace
11. Workforce
12. Information Management
13. Information Technology
14. Asset Management
15. Project Management
16. Procurement
17. Financial Management and Control
18. Internal Audit
19. Security and Business Continuity
20. Citizen-focussed Service
21. Alignment of Accountability Instruments

Rating Scale
Strong
Acceptable
Opportunity for Improvement
Attention Required

AoM 19 – Description and Lines of Evidence

19. Effective Management of Security and Business Continuity

Security and business continuity contribute to the effectiveness of government by safeguarding employees, information, and assets and ensuring the continued availability of critical services

No change since MAF V

Lines of Evidence:

19.1 DEPARTMENTAL SECURITY PROGRAM:

Focus of this training session

Extent to which a departmental security program is established and managed based on the *Government Security Policy (GSP)* to ensure the co-ordination of all policy functions and implementation of policy requirements.

19.2 MANAGEMENT OF INFORMATION TECHNOLOGY SECURITY (MITS):

Extent to which an Information Technology (IT) security program is established and managed based on the *MITS Operational Security Standard* on to ensure that sensitive information and IT systems are adequately protected.

19.3 BUSINESS CONTINUITY PLANNING (BCP) PROGRAM:

Extent to which a BCP program is established and managed based on the *BCP Program Operational Security Standard* to ensure that measures are in place to provide for the continuity of critical services.

AoM 19 – Rating Criteria

No change since MAF V

MAF Rating	Colour Rating	Criteria
Strong	Blue	At least one line of evidence at the *Strong* category and no line of evidence below *Acceptable* equates to an overall rating of *Strong.*
Acceptable	Green	At least two lines of evidence at or above the *Acceptable* category and no line of evidence below *Opportunity for Improvement* equates to an overall rating of *Acceptable.*
Opportunity for Improvement	Yellow	At least two lines of evidence at the *Opportunity for Improvement* category and no line of evidence below *Opportunity for Improvement* (or one line of evidence at the *Attention Required* category and two lines of evidence at or above *Acceptable*) equates to an overall rating of *Opportunity for Improvement.*
Attention Required	Red	Two or more lines of evidence at the *Attention Required* category (or one line of evidence at the *Attention Required* category and one or both other lines below the *Acceptable* category) equates to an overall rating of *Attention Required.*

19.1 Departmental Security Program - Overview

- **Compliance with the GSP, as substantiated by evidence provided by departments and agencies**

- **Assessed elements:**

Minor change since MAF V (see note)

  - **Security organization and program governance**
    - DSO appointment and positioning
    - Security organization and governance
    - Security program and coordination mechanisms

  - **Other assessed elements**
    - Sharing of information and assets with organizations outside the federal government
    - Security training
    - Security awareness
    - Security briefings
    - Incident management

  - **For strong rating:** leadership and contribution to GC-wide security program, and alignment and integration of security strategy with corporate priorities and business plan

Note: "Security in increased threat and emergency situations" was assessed but not rated in MAF V, and will not be assessed in MAF VI.

New in MAF VI

- **Overview document** describing security policy compliance and management performance for each assessed element, and guiding TBS analysts through supporting evidence (prepared using standardized response template)
  - **Also includes information related to the other lines of evidence (19.2 and 19.3)**
- Focus assessment on **changes** since MAF V and allow **reuse** of evidence submitted in Round V
- **Maximum of 50 evidentiary documents** can be submitted for 19.1 (a total of 60 for the area of management, including the overview document, MITS questionnaire and updates)
  - ***** No embedded documents**
- **(For Strong rating)** Description of GC-wide leadership and alignment of security program with business priorities and plans (was part of criteria in MAF V but no evidence was requested)
- **(For information only - will not affect rating)** Identification if compliance and performance have been independently validated, e.g. through performance measurement, internal audit or evaluation

19.1 Rating Scale

No change since MAF V

MAF Rating	Colour Rating	Criteria—LoE 1 (Departmental Security Program)
Strong	Blue	Organization fully satisfies all the Security Organization and Program Governance requirements, and meets most or all requirements for the other assessment areas, and there are no significant deficiencies. Organization demonstrates leadership and contributes to the government-wide security program. Organization's security strategy is aligned and integrated with its corporate priorities and business plan.
Acceptable	Green	Organization fully satisfies all the Security Organization and Program Governance requirements and most elements of the other assessment areas, and there are no significant deficiencies.
Opportunity for Improvement	Yellow	Organization fully satisfies most of the Security Organization and Program Governance requirements and some elements of the other assessment areas.
Attention Required	Red	Failure to satisfy most of the requirements related to Security Organization and Program Governance or significant deficiencies in most elements of the other assessment areas will result in an Attention Required rating for this line of evidence.

19.1.1 Security Organization and Program Governance (1)

Analytical Approach	Supporting Evidence
i) Has a DSO been appointed? If a DSO has not been appointed or if an acting DSO has been appointed, are there plans to permanently staff the position?	• Title, classification, and appointment status of DSO • (If DSO has not been appointed or acting DSO) Plans to permanently staff the DSO position
ii) Is the DSO strategically positioned in the organization, to provide advice and guidance to senior management?	• Reporting relationship between the DSO and senior management • Mechanisms used by DSO to engage and advise senior management in managing security risks

Additional Guidance

- Examples of mechanisms used to engage and advise the departmental executive: regular participation in senior management committees, regular and ad hoc briefings or management reports

19.1.1 Security Organization and Program Governance (2)

Analytical Approach	Supporting Evidence

iii) Is there a security organization with established governance, key security positions, and well defined roles and responsibilities to ensure effective management of the security program?	Organizational chart or equivalent document describing:
	• Security positions and reporting relationships
	  • **For all elements of the departmental security program (including personnel screening, physical security, IT security, security in contracting and BCP)**
	  • **Between the security organization and other groups with security responsibilities (e.g., HR, IT, IM)**
	
	Departmental security governance structure, such as:
	• Terms of reference of committees
	• Roles and responsibilities (e.g. from departmental security policy)
	• Memorandum Of Understanding (MOU) or other arrangement to govern provision of security services by a third party, such as a portfolio department or shared services provider

Additional Guidance

- Where security services are provided by a third party (including another department), evidence needs to demonstrate **clear accountabilities and responsibilities** for all elements of the departmental security program
- Should illustrate relationships to groups with responsibilities related to security, such as emergency preparedness and occupational health and safety
- Should include an estimate of the number of Full Time Equivalents (FTEs) allocated to security and corresponding salary budget, and classification of key security positions

19.1.1 Security Organization and Program Governance (3)

Analytical Approach	Supporting Evidence
iv) Is there a departmental security program in place that ensures coordination and implementation of key policy requirements?	Examples of departmental security strategies, policies and work plans addressing key policy functions (i.e. personnel screening, physical security, IT security, security in contracting and BCP)

Additional Guidance

- When security policies from another organization have been adopted for use within the department, evidence is needed that documents the decision to adopt the policies and any adaptation to them

19.1.2 Sharing of Information and Assets (1)

Analytical Approach

- Are measures in place to establish agreements (e.g. MOUs) for sharing information or assets with organizations outside the federal government (outside of a contractual context)?
- Do agreements include security responsibilities, safeguards, and terms and conditions for continued participation?
- Are sharing agreements regularly monitored to verify compliance with security requirements, and periodically reviewed to confirm their status and relevance?

Supporting Evidence

- Departmental policy requirements, and roles and responsibilities related to sharing of information and assets
- Practices and procedures related to the establishment, monitoring, and review of agreements, such as:
  - Standard security clauses for agreements
  - Mechanisms used to ensure the inclusion of security clauses in agreements
  - List of agreements currently in place
  - Representative example of a sharing agreement including security clauses

19.1.2 Sharing of Information and Assets (2)

Additional Guidance

- Assessment area pertains solely to **non-contractual** arrangements with organizations **outside** the federal government (i.e. for whom the GSP does not apply)

- If the organization **does not currently share** any information or asset with organizations outside the federal government:
  - This should be stated in the overview document
  - There should be measures in place to establish agreements in the event such sharing were to occur in the future

- Evidence should highlight the **involvement of the DSO** and other security officials, and the **responsibilities of other managers** in the establishment, monitoring, and review of agreements
  - Measures used to ensure the inclusion of security provisions in sharing agreements do not necessarily involve the review by security officials of each sharing agreement, as other mechanisms may be used to ensure policy compliance

19.1.3 Security Training (1)

Analytical Approach

- Are measures in place to ensure that individuals who have specific security duties receive appropriate, up-to-date training?

Supporting Evidence

- Departmental policy requirements, and roles and responsibilities related to security training
- Practices and procedures related to security training, such as:
  - Competency profiles and training curriculum for key security positions
  - Professional designations held by departmental staff responsible for security
  - Summary of security training attended in the last year
  - Level of investment in security training
  - Approaches for measuring implementation and effectiveness of security training program

19.1.3 Security Training (2)

Additional Guidance

- Assessment area pertains solely to **specialized security training** received by security managers and specialists, or other individuals with specific security duties (e.g. human resources staff and managers with responsibilities for personnel screening)

- Evidence may also be provided if security training is provided to **other individuals** with more general security responsibilities (e.g. managers with responsibilities for managing security risks related to their program)

- Evidence related to a general security awareness program targeting all employees, or to other types of training (e.g. emergency preparedness, occupational health and safety) is **not relevant** to this assessment area
  - The overview document may describe the coordination and integration of security training with other types of training.

- No personal information is to be submitted

19.1.4 Security Awareness (1)

Analytical Approach

- Is there a security awareness program to inform and regularly remind individuals of their security responsibilities address issues and concerns?

Supporting Evidence

- Departmental policy requirements, and roles and responsibilities related to security awareness

- Practices and procedures related to security awareness, such as:
  - Awareness strategy
  - Summary of awareness activities conducted in the last year
  - Summary of awareness material currently in place
  - Sample awareness material
  - Level of investment in security awareness
  - Approaches for measuring implementation and effectiveness of security awareness program

19.1.4 Security Awareness (2)

Additional Guidance

- Assessment area pertains solely to awareness measures related to **security**
- Evidence related to other types of awareness measures (e.g. emergency preparedness, occupational health and safety) is **not relevant** to this assessment area
  - The overview document may describe the coordination and integration of security awareness with other types of awareness.

19.1.5 Security Briefings (1)

Analytical Approach

- Are measures in place, as part of the personnel screening process, to ensure that individuals:
  - Are formally briefed on the access privileges and prohibitions attached to their screening level prior to commencement of duty (or when required in the update cycle)?
  - Sign the appropriate briefing forms?

Supporting Evidence

- Departmental policy requirements, and roles and responsibilities related to security briefings

- Practices and procedures related to the execution of security briefings for new employees as part of the personnel screening process, such as:

  - Procedures for briefing individuals when granting a reliability status or security clearance

  - Briefing form used

  - Procedures for updates (e.g. when there is a change in reliability status or security clearance level)

19.1.5 Security Briefings (2)

Additional Guidance

- Assessment area pertains solely to the **formal** security briefings conducted in the context of the personnel screening process
- Evidence related to the general security awareness briefings provided to all employees is **not relevant** to this assessment area
- Evidence provided should not include any personal information

19.1.6 Incident Management (1)

Analytical Approach

- Are measures in place to ensure that security incidents are reported and investigated, and corrective action taken in a timely, coordinated, and effective manner?

Supporting Evidence

- Departmental policy requirements, and roles and responsibilities related to incident management
- Practices and procedures for managing security incidents, such as:
  - Incident management plan and concept of operations
  - Procedures for reporting incidents internally within the department or agency and externally to central and lead security agencies, and where appropriate to law enforcement authorities
  - Procedures or guidelines for conducting administrative investigations of security incidents
  - Procedures for applying corrective actions

19.1.6 Incident Management (2)

Additional Guidance

- Assessment area pertains solely to the management of **security incidents**
- Evidence pertaining to emergency preparedness (e.g. building evacuation plans), although related, is **not relevant** to this assessment area
- Procedures and other evidence submitted collectively need to cover the management of **all types** of security incidents that are within the scope of the GSP, including:
  - Threats or acts of violence toward an employee
  - Asset theft, loss or destruction
  - Compromise of sensitive information
  - IT security related incidents
  - Disruption of critical services
  - Other events with a real or potential impact on security

19.2 Management of IT Security (MITS)

- **Compliance with the MITS standard, as determined by departmental self-assessment**

- **Assessed elements**

No change since MAF V

  - **MITS priority objectives**
    - ITS fundamentals (people, processes, strategies, organization, risk management program)
    - Identification and securing of critical systems
    - Senior management engagement in management of IT security risks
  - **MITS requirements**
    - IT security organization
    - ITS policy
    - ITS resources and system development lifecycle
    - Identification of assets
    - Risk management
    - Incident management
    - Vulnerability management
    - Continuity planning
    - Audit, monitoring and assessment
    - Awareness
    - Other technical and operational safeguards
  - **For strong rating:** leadership and contribution to GC-wide IT security program

New in MAF VI

- Organizations are encouraged to provide **supporting information** in the MITS questionnaire, to provide context to, and improve interpretation of the responses
- Focus assessment on **changes** since MAF V
- **(For Strong rating)** Description of leadership and contribution to GC-wide IT security program (was part of criteria in MAF V but no evidence was requested)
- **(For information only - will not affect rating)** Identification if compliance and performance have been independently validated, e.g. through performance measurement, internal audit or evaluation

19.2 Rating Scale

No change since MAF V

MAF Rating	Colour Rating	Criteria—LoE 2 (Management of Information Technology Security)
Strong	Blue	Organization fully satisfies the three priority objectives and complies with MITS minimum requirements, and demonstrates leadership and contributes to the government-wide IT security program.
Acceptable	Green	Organization satisfies the three priority objectives and has most or all of the MITS requirements in place, and there are no significant deficiencies.
Opportunity for Improvement	Yellow	Organization satisfies the three priority objectives and has some of the MITS requirements in place, however significant deficiencies remain.
Attention Required	Red	Organization did not satisfy the three priority objectives.

19.3 Business Continuity Planning (BCP) Program

- **Compliance with the BCP Program standard, as determined by departmental self-assessment**

- **Assessed elements**

No change since MAF V

  - **BCP Program Governance**
    - Establishment of authorities and responsibilities for BCP program
  - **Business Impact Analysis**
    - Identification and prioritization of critical services and assets
  - **BCP Plans and Arrangements**
    - Measures to ensure continued availability of critical services and assets
  - **BCP Readiness**
    - Review, testing and audit of plans and on-going monitoring of readiness

  - **For strong rating:** readiness plans for pandemic influenza and IM/IT emergency preparedness

New in MAF VI

- **BCP Program Compliance Report** (formerly known as Action Plan Template), developed by Public Safety in consultation with TBS (minor changes from MAF V to clarify questions)
- Compliance Report submitted directly to Public Safety **(*** no other evidence required***)**
- Focus assessment on **changes** since MAF V
- Organizations are encouraged to provide **supporting information** in the BCPP Compliance report, to provide context to, and improve interpretation of the responses
- **(For information only - will not affect rating)** Identification if compliance and performance have been independently validated, e.g. through performance measurement, internal audit or evaluation

19.3 Rating Scale

No change since MAF V

MAF Rating	Colour Rating	Criteria—LoE 3 (Business Continuity Planning Program)
Strong	Blue	Organization fully satisfies all BCP program requirements, and has completed and approved readiness plans for pandemic and IM/IT emergency preparedness.
Acceptable	Green	Organization fully satisfies all of the BCP Program Governance and Business Impact Analysis requirements; BCP Plans and Arrangements are completed and approved by senior management; establishment of a maintenance cycle is in progress or completed; and there are no significant deficiencies.
Opportunity for Improvement	Yellow	Organization fully satisfies all of the BCP Program Governance requirements and some elements of Business Impact Analysis, and the establishment of BCP Plans and Arrangements is in progress.
Attention Required	Red	Failure to satisfy all the requirements related to the establishment of BCP Program Governance, non-completion of a BIA or lack of plans to conduct one, or significant deficiencies in most elements of the BCP Program standard will result in an Attention Required rating for this line of evidence.

AoM 19 Response Template ("Overview Document")

Purpose

- This document is intended to summarize the required information for AoM 19 and provide a reference to the applicable evidence for each assessment element
  - Help departments create a complete submission package
  - Focus assessment on changes since round V and allow reference to evidence submitted in round V
  - Guide TBS analysts in the review of supporting evidence

Content

- The template contains 8 sections:
  - **Page 1 :** Document Description
  - **Page 2** : Instructions
  - **Page 3:** Document Inventory (for 19.1)
  - **Part A :** 19.1 Departmental Security Program
  - **Part B :** 19.2 MITS and 19.3 BCP Program
  - **Part C :** Assessment elements for "Strong" rating (19.1 and 19.2)
  - **Part D :** Performance measurement, internal audits, management reviews, evaluations, etc.
  - **Part E :** Additional information

Document Description and Document Inventory

Document Description	
Organization Name	
Departmental MAF contact	
Prepared by	
Approved by	
Approval date	
Submission type	
Description of changes	

Reuse from Round V

Sharing best practices

Document Inventory (Line of Evidence 19.1)

Ref #	Document Name *(file name if electronic)* *(For embedded documents submitted in MAF Round V: please also identity the document in which the document was embedded)*	Document Description *(if document name not self-explanatory)*	MAF Round *(V or VI)*	Submission Method *(Portal, hard copy, CD, email)*	Assessment Element(s) *(e.g. 19.1.1 (i))*	Share? *("Yes" indicates consent to share)*
1						
…						
50						

Maximum:
- 50 documents (19.1)
- Portal: up to Protected A

Part A: Departmental Security Program

Add reference(s) if applicable
Maximum 10 references per element
Can include references to documents submitted for other AoMs or regular sources (e.g. RPP, DPR)

Part A - Line of Evidence 19.1 Departmental Security Program

#	Assessment Element	Description *(Please refer to the Evaluation Methodology and Guide for evidence requirements and analytical approach)*	Reference to Applicable Evidence *(Please include reference number (#) from inventory, document name and applicable section(s))*	Changes since MAF Round V or since last update submitted *(if applicable)*	Activities, plans and timelines for improving performance
19.1.1	Security organization and program governance	*i. DSO appointment*			
…	…	…			

Add narrative describing departmental compliance and performance

Describe changes since MAF Round V

Part B: 19.2 MITS and 19.3 BCP Program

Revise if update submitted during Round V

Part B - Lines of evidence 19.2 and 19.3				
#	**Element**	**Questionnaires** *(Please identify the date of the document that was submitted for the MAF Round VI assessment)*	**Changes since MAF Round V or since last update submitted** *(if applicable)*	**Activities, plans and timelines for improving performance**
1.	**Management of Information Technology Security (MITS)**	**MITS Questionnaire Dated:** ***Note:*** *The completed MITS questionnaire needs to be submitted directly to the Secretariat, preferably using the MAF portal.*		
2.	**Business Continuity Planning (BCP) Program**	**BCP Program Compliance Report Dated:** ***Note:*** *The completed BCP Program Compliance Report needs to be submitted* ***directly to Public Safety Canada****. Your BCP Manager can contact your departmental contact at Public Safety Canada for details regarding submission of completed templates.*		

Describe changes since MAF Round V

Describe changes since MAF Round V

Part C: Elements for Strong Rating

Optional

Part C - Assessment elements for strong rating
(Lines of evidence 19.1 and 19.2)

#	Assessment Element	Description	Reference to Applicable Evidence *(optional)*	Changes since MAF Round V or since last update submitted *(if applicable)*	Activities, plans and timelines for improving performance
1.	**Leadership and extra-organizational contributions**				
2.	**Strategic alignment**				

Add description of the leadership and contributions of the organisation to the government-wide security program (whether it is for the entire program or for a specific element such as IT security or BCP)
***Does not include** leadership and contributions of organisations with mandated government-wide responsibilities for security ***

Add description of how the organisation's security strategy is aligned and integrated with its corporate priorities and business plans

Part D: Performance Measures, etc., and E: Additional Information

Part D - Performance measurement, internal audits, management reviews, evaluations and other assessments conducted in the past 5 years or planned *(All lines of evidence – unrated element)*					
#	**Type** *(e.g. performance measurement, internal audit, management review, evaluation)*	**Description** *(Brief description of purpose of assessment, how it was conducted, participants, frequency, etc.)*	**Scope** *(Identification of security program element, system, organizational unit, program, service, etc. within the scope of the assessment)*	**Date conducted or planned**	**Additional information** *(Available reports, action plans, etc.)*
1.					
...					

Optional
(may contribute to Strong assessment)

Part E - Additional information *(e.g. significant barriers to progress, suggestions regarding the MAF process for this area of management)*

Optional

Additional Guidance

AoM 19 Evaluation Methodology and Guide

- Details the evidence requirements, analytical approach and rating criteria for each line of evidence
- Provided via email to departmental MAF Coordinators, DSOs and IT Security Coordinators

Stewardship element of the MAF

- For more information on the Stewardship element of the MAF and related areas of management, see:

http://publiservice.tbs-sct.gc.ca/maf-crg/indicators-indicateurs/2008/stewardship-gerance/stewardship-gerance-eng.asp

Public Safety Canada

- For guidance on the BCP Program Compliance Report, please contact your BCP Quality Assurance representative or the BCP helpdesk:

E-mail: bcp.helpdesk@ps-sp.gc.ca

Telephone: 613.949.6522

Website: http://bcp.ps.gc.ca

Future Years

Assessment methodology matured and broadened to:

- Align with the new *Policy on Government Security* and associated Directives and Standards
- Assess other aspects of departmental security programs (e.g. personnel screening, security in contracting, physical security, information security)
- Include identity management
- Measure effectiveness and value (vs compliance)
- Leverage departmental performance measurement

TBS Contacts

Pierre Boucher
AoM 19 Lead
Email: Pierre.Boucher@tbs-sct.gc.ca
Telephone: 613-952-0169

Nathalie Pelletier
Primary contact for AoM 19, the new response template and 19.1
Email: Nathalie.Pelletier@tbs-sct.gc.ca
Telephone: 613-952-2906

Brian Brazeau
Primary contact for 19.2 and 19.3
Email: Brian.Brazeau@tbs-sct.gc.ca
Telephone: 613-957-2549

Samantha Tim
Analyst for 19.1
Email: Samantha.Tim@tbs-sct.gc.ca
Telephone: 613-960-1066

*** ***Important notes:***

- For matters related to the BCPP Compliance Report for 19.3, please contact your BCP QA representative at Public Safety Canada
- Please keep your departmental MAF coordinator informed of all communications regarding MAF

Questions ?