Management Accountability Framework (MAF)

Evaluation Methodology and Guide

Round VI (2008-09)

11 September 2008

Area of Management 19: Security and Business Continuity

Treasury Board of Canada Secretariat
Chief Information Officer Branch
Security and Identity Management Division

Area of Management Lead: Pierre Boucher, Senior Director, SIDM

I—INTRODUCTION

The Management Accountability Framework (MAF) sets out the Treasury Board's expectations of senior public service managers for good public service management. The MAF defines the conditions that need to be in place to ensure government is well-managed and to promote management excellence. The MAF process includes annual assessments of most departments and agencies, engagement between deputy heads and the Treasury Board of Canada Secretariat (the Secretariat) and the Canada Public Service Agency where warranted, joint agreement on specific management improvement action plans and ultimately public reporting on the state of management. The government uses MAF assessments to identify management strengths and weaknesses in individual departments and agencies and ultimately on a government-wide basis.

The MAF is structured around 10 integrated elements that collectively define "management" and establish the expectations for good management of a department or agency. Each of these elements is supported by a statement that defines the related management expectation, and a set of “areas of management” that convey the breadth and meaning of the management expectation. These areas of management are the basis for data gathering and analysis related to each of the MAF elements, and for conducting the annual MAF assessments.

One of the MAF elements, *Stewardship*, sets expectations for the establishment of an effective and integrated departmental control regime (assets, money, people, services, etc.), and for ensuring that its underlying principles are clear to all staff. By MAF Round IV in fiscal year 2006-2007, it was apparent that an effective control regime requires that departments and agencies effectively manage security and business continuity to support Government’s objectives and the national interest. A new area of management was established in Round V under the *Stewardship* element to set expectations and assess departmental performance related to security and business continuity.

Responsibility for Preparing for a MAF Assessment

Managers are responsible for demonstrating through their MAF submission the effectiveness of their departmental or agency security program, under the leadership of the Departmental Security Officer (DSO)[1].

This document provides guidance to assist managers in preparing their submissions for the Security and Business Continuity area of management. Section II provides general information on the sources of evidence and describes how the MAF ratings will be determined for this area of management. This section also provides an overview of changes from MAF Round V and anticipated future changes. Section III contains a description of the lines of evidence against which departments and agencies will be assessed. For each line of evidence, section III describes the evidence that departments and agencies need to submit to support the MAF assessment, the analytical approach that will be used to assess departmental or agency performance, and the scale that will be the basis for assigning ratings. Informative notes are provided throughout this section to assist managers in preparing a complete submission. Together, this guidance is expected to assist managers in preparing high quality submissions as well as inform them of how their submission will be assessed. Section IV provides a summary of the evidence requirements for this area of management and can be used as a checklist to validate the completeness of a submission.

[1] Or Agency Security Officer (ASO), as applicable.

Responsibility for Assessing Security and Business Continuity under the MAF

The Security and Identity Management (SIDM) Division, Chief Information Officer Branch (CIOB), is responsible for the Security and Business Continuity area of management, which includes the Government Security Policy (GSP) and Management of Information Technology Security (MITS) assessments. The SIDM Division is also responsible, in conjunction with Public Safety Canada, for the Business Continuity Planning (BCP) Program[2] assessments.

The SIDM Division will use the evidence provided by managers to assess departmental or agency performance in relation to the Security and Business Continuity area of management. The following three lines of evidence will be examined for this area of management:

AREA OF MANAGEMENT 19: 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, as measured by:

LINE OF EVIDENCE 19.1: Departmental Security Program (DSP)

Extent to which a departmental security program is established and managed based on the GSP to ensure the coordination of all policy functions and implementation of policy requirements.

LINE OF EVIDENCE 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 to ensure that sensitive information and IT systems are adequately protected.

LINE OF EVIDENCE 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.

Key Relevant Policy Instruments

The following policy instruments serve as the policy foundation upon which the SIDM division will conduct its assessment for Area of Management 19:

Government Security Policy
Operational Security Standard: Management of Information Technology Security
Operational Security Standard: Business Continuity Planning Program

[2] In some references, the term Business Continuity Management (BCM) Program is used and has the same meaning as BCP Program.

II—SOURCES OF EVIDENCE AND AREA OF MANAGEMENT RATING

Evidence—General

The MAF methodology requires that data and evidence used in conducting assessments be generally obtained from sources that the Secretariat uses to assess departmental or agency performance through its normal oversight activities. These sources include: Estimates (Annual Reference Level Updates, Reports on Plans and Priorities (RPPs), Departmental Performance Reports (DPRs)), Management, Resources, and Results Structure Policy, Program Activity Architectures, Memoranda to Cabinet, Treasury Board Submissions, and Records of Decision. Assessments may also draw on information exchanged during ongoing engagement of departments and agencies in the form of consultation and advice, discussion of Treasury Board Submissions, and participation in various forums and committees.

In addition to these regular sources of data, the SIDM Division will use the evidence and analytical approach specified in the **Methodologies** section of this Guide (section III) to assess departmental or agency performance related to this area of management.

If required, SIDM will clarify information with the department or agency and also use other sources of evidence—internal audits, audits and reviews conducted by the Office of the Auditor General (OAG) or the Secretariat, and departmental web sites—to evaluate departmental policy compliance and management performance.

Area of Management Rating

The Secretariat developed a standardized MAF rating guide, associating a distinct colour rating with respective criteria that must be met. Departments and agencies are assessed according to whether they meet the criteria as set out in each line of evidence. The overall rating for the area of management is based on the ratings obtained for each line of evidence.

Ratings for Area of Management 19 will be determined according to the following scale:

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.*

Changes from Round V

No significant changes have been made from Round V to Round VI with respect to evidence requirements, analytical approach, or rating criteria for Area of Management 19. However minor adjustments were made to the evaluation methodology to clarify the evidence requirements, analytical approaches, and assessment process. These changes are reflected throughout this Guide.

Important change : Although departments and agencies did not have to provide an overview document in MAF Round V for Area of Management 19, most organizations provided a description of their compliance and performance level to help guide the Secretariat analysts through the evidence submitted. Submission of an overview document is now required in MAF Round VI, as described in the **Methodologies** section of this Guide (section III). Details are contained in the new response template for this area of management. It should be noted that the response template is provided as a separate document to this Guide.

For organizations that were assessed in MAF Round V, the assessment in Round VI will focus on changes made from last year. Organizations should highlight these changes in the overview document and in their MITS questionnaire and BCP program compliance report.

Assessments in future years

The methodology in future years will be aligned with the requirements set out in the revised Policy on Government Security and related directives and standards. As the MAF process matures, so will methodologies to assess the effectiveness of departmental security activities and achievement of results.

Additionally, the Secretariat may assess the extent to which departments and agencies have implemented measures to address security management areas not currently covered by the methodology, including:

- Personnel screening
- Physical security
- Security in contracting
- Identity management

III—METHODOLOGIES

This section describes the evidence requirements, analytical approach and rating criteria for the three lines of evidence of Area of Management 19. Evidence provided need to demonstrate effective management of security and business continuity in a department or agency.

Line of Evidence 19.1: Departmental Security Program

Extent to which a departmental security program is established and managed based on the GSP to ensure the coordination of all policy functions and implementation of policy requirements.

1. **Evidence: Overview document and departmental security program documents**

The Government Security Policy requires that departments and agencies appoint a DSO to establish and manage a security program that ensures coordination of all policy functions and implementation of policy requirements. Departments and agencies are requested to provide the Secretariat with the following evidence to support the MAF assessment for this line of evidence:

a. Overview document:

   A document describing departmental security activities, policy compliance, and management performance for each assessed element described in section 2 (**Analytical approach**) and guiding the Secretariat analysts in the review of evidence submitted. For each assessed element, this document needs to include a cross-reference to the applicable evidence document(s) submitted and relevant section(s) within them. The overview document should also capture action plans and timelines for addressing known deficiencies and improving performance. For those organizations that were assessed in MAF Round V, the overview document should also identify areas of improvement and other changes from last year.

   - ***Note**: This overview document is to be prepared using the template provided as a separate attachment to this Guide.*

b. Evidence related to the management of the following areas of the departmental security program:

   - *19.1.1 Security Organization and Program Governance*:
     - i) DSO appointment: Identification of DSO official title, classification, and appointment status (or staffing plans if the position is empty or under an acting assignment)
     - ii) DSO strategic positioning: Description of reporting relationship between the DSO and the departmental executive
       - ***Note:** The overview document should include a description of mechanisms that the DSO uses (including use of committees, regular and ad hoc briefings or management reports) to engage and advise the departmental executive in the management of security risks.*
     - iii) Security organization and governance:
       - Organizational chart or equivalent document showing or describing security positions (including dedicated and part-time resources) and reporting relationships within the security organization and between the security organization and other groups with responsibilities related to security

         Notes:

         - *Positions and reporting relationships for all elements of the departmental security program need to be shown or described, including personnel screening, physical security, IT security, security in contracting and BCP.*

- *Relationships to groups with responsibilities related to security, such as emergency preparedness and occupational health and safety, should also be depicted.*
- *The overview document should include an estimate of the number of Full Time Equivalents (FTEs) allocated to security and corresponding salary budget. The classification of key security positions should also be indicated.*

o Departmental security governance structure (e.g. terms of reference of committees; roles and responsibilities; coordination mechanisms between the DSO and the departmental executive, within the security organization, and between the departmental security organization and other groups for security program activities; 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)

Notes:

- *A separate document describing roles and responsibilities for departmental security is not necessarily required, as these may be defined in departmental security policies provided in support of the following evidence requirement.*
- *Where security services are provided by a third party, evidence submitted needs to demonstrate clear accountabilities and responsibilities for all elements of the departmental security program. While some responsibilities may be delegated to a third party, accountability for ensuring the security of its people, information, and assets and the continuity of its services rests with the department or agency.*

- iv) Departmental security program: Departmental security strategies, policies and work plans addressing key policy functions (i.e. personnel screening, physical security, IT security, security in contracting and BCP)

Notes:

- *Departmental security policies provide evidence in support of the Security Organization and Program Governance assessment element, but may also identify departmental policy requirements, roles and responsibilities, and practices in support of the evidence requirements pertaining to each of the assessment elements described below (e.g. Sharing of information and assets, Security training). Where this is the case, the overview document needs to identify for each assessment element the section within the policy where the required evidence can be found.*
- *When security policies from another organization have been adopted for use within the department or agency (including policies issued by Treasury Board), evidence is needed that documents the decision to adopt the policies and any adaptation to them (e.g. alignment of roles and responsibilities defined in the policy to the organizational structure and security governance, adaptation of policy requirements to the organizational context or to unique security requirements).*

- *19.1.2 Sharing of information and assets*: Departmental policy requirements, roles and responsibilities, and practices and procedures related to the establishment, monitoring, and review of agreements related to the sharing of information or assets with organizations outside the federal government (e.g. 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)

***Notes**:*

- *This assessment area pertains solely to **non-contractual** arrangements with organizations **outside** the federal government. Agreements with other federal institutions or contractual arrangements are **not** relevant to this assessment element.*
- *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. It should be noted that 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.*
- *If the organization does not currently share any information or asset with organizations outside the federal government and outside of a contractual context, this fact should be stated in the overview document. Measures should nevertheless be in place to ensure that agreements are established in the event that such sharing would occur in the future.*

- *19.1.3 Security training*: Departmental policy requirements, roles and responsibilities, and practices and procedures related to the training of individuals with specific security duties (e.g. competency profiles and training plans for key security positions, professional designations held and summary of security training attended in the last year by security managers and specialists, level of investment in security training, approaches for measuring implementation and effectiveness of security training program)

  ***Notes**:*

  - *The focus of this assessment area is **specialized security training** received by security managers and specialists, or other individuals with specific security duties (e.g. human resources 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 (such as occupational health and safety, and emergency preparedness) is not deemed relevant to this assessment area. The overview document may however describe the coordination and integration of security training with other types of training.*
  - *Evidence provided should not include any personal information.*

- *19.1.4 Security awareness*: Departmental policy requirements, roles and responsibilities, and practices and procedures related to security awareness (e.g. 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)

  - ***Note**: This assessment area pertains solely to awareness measures related to security. Evidence related to other types of awareness measures (e.g. emergency preparedness) is not deemed relevant to this assessment area. The overview document may however describe the coordination and integration of security awareness with other types of awareness activities.*

- *19.1.5 Security briefings*: Departmental policy requirements, roles and responsibilities, and practices and procedures related to the execution of security briefings for new employees as part of the personnel screening process (e.g. procedures for briefing individuals when granting a reliability status or security clearance, procedures for updates, briefing form used)
    - ***Note**: This 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 deemed relevant to this assessment area. Evidence provided should not include any personal information.*

- *19.1.6 Incident management*: Departmental policy requirements, roles and responsibilities, and practices and procedures for managing security incidents (e.g. 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 for conducting administrative investigations of security incidents; and procedures for applying corrective actions)

    Notes

    - *This assessment area focuses solely on the management of security incidents. Evidence pertaining to emergency preparedness (e.g. building evacuation plans), although related, is not deemed 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; and other events with a real or potential impact on security).*

c. Information related to elements assessed for the Strong rating:

- *Leadership and extra-organizational contributions:* the overview document should include a description of how the organization provides leadership and contributes to the government-wide security program (whether for the security program as a whole or for a specific element such as IT security). Supporting evidence can also be provided but is not required for this element.
    - ***Note**: This description will also be used to support the Strong rating assessment for 19.2 (MITS). This assessment element **does not** include the leadership and contributions of organizations in the context of their mandated government-wide responsibilities for security (e.g. leadership and contributions of Royal Canadian Mounted Police for physical and IT security, Public Works and Government Services Canada for security in contracting, Communications Security Establishment for IT security, Canadian Security Intelligence Service for security screening, and Public Safety Canada for BCP and incident management).*
- *Strategic alignment:* The overview document should also include a description of how the organization's security strategy is aligned and integrated with its corporate priorities and business plan. Supporting evidence can also be provided but is not required for this element.

d. Information related to performance measurement, internal audit, management reviews, evaluations and other types of assessments of security program:

In MAF Round VI, departments and agencies are also requested to identify in the overview document whether the current level of policy compliance and management performance for the departmental security program, as reported in the overview document for line of evidence 19.1 and in the questionnaires submitted for lines of evidence 19.2 and 19.3, have been validated through performance measurement, internal audit, management review, evaluation or another assessment in the last five (5) years (or if such validation is planned for). For each validation conducted or planned, the overview document should identity the type of validation (e.g. performance measurement, internal audit, management review, evaluation, external audit, third

party review), the scope of the validation (e.g. entire security program, IT security, security in contracting, BCP program, specific system) and the date the validation was conducted (or is planned). Available reports or action plans resulting from this validation should also be identified. This information will be used by the Secretariat to determine the current level of coverage for performance measurement, internal audits, management reviews, evaluations and other assessments related to security, and will **not** affect a department or agency's MAF assessments or ratings.

Notes:

- *For each assessment element, the overview document needs to include a reference to the document(s) submitted to meet the evidence requirements described in the previous sections. Evidence may also be included directly in the description column of the overview document (e.g. identification of DSO title, classification, and staffing status).*

- *Departments and agencies may also refer to regular sources such as RPPs and DPRs for evidence related to the management of security and business continuity. These regular sources, if applicable to this area of management, should also be included in the inventory and referred to in the overview document, in the relevant assessment element*

- *Departments and agencies that were assessed in MAF Round V may reuse evidence that was submitted last year. For documents that were submitted electronically through the MAF portal, departments and agencies need to identify, in the overview document, the file name of the document that they wish to reuse (as it appears on the MAF portal) and the area of management for which the document was submitted (if submitted for another area of management), and provide a description of the document if the file name is not self-explanatory. For documents submitted by other means, departments and agencies need to identify the method by which the document was submitted, the format (e.g. hard copy, CD, email) and the file name (for electronic documents), and provide a description of the document. Additionally, for all documents, departments and agencies need to identify the sections that pertain to the element being assessed.*

- *The overview document and other evidence submitted electronically for this line of evidence **must not contain any embedded documents**. Each document needs to be submitted under a separate cover and appropriately referenced in the overview document. Any embedded documents submitted will not be considered in the assessment for this area of management (except for those previously submitted for MAF Round V when this constraint was not enforced).*

- *The evidence submitted in support of the MAF assessment for this Line of Evidence **must not exceed 50 documents**. This maximum number includes both the documents submitted in MAF Round VI and documents submitted in MAF Round V that are identified for reuse in the inventory included in the overview document. In general however, fewer documents should be required to demonstrate policy compliance and management performance.*

- *To reduce the number of documents submitted as evidence, a summary or list of departmental or agency security initiatives (e.g. sharing agreements, awareness material) should be submitted, accompanied by one or a few representative samples instead of multiple samples of similar evidence.*

- *All documents submitted as evidence need to be official (i.e. bear the identification of the organization being assessed, be approved and current). Draft material may be submitted, provided that planned dates for approval are given in the overview document. Where the planned date for approval falls outside of the assessment period for MAF Round VI, partial compliance may be determined. Material originating from another organization may be submitted, provided that there is also evidence demonstrating its current application within the organization being*

assessed (e.g. official memo documenting adoption of a particular standard, procedure or guideline).

2. **Analytical approach:**

Evaluations will be based on the extent to which the departmental security program is established, managed, and administered by the security organization through program governance, strategies, work plans, policies, procedures, and practices.

The following elements will be assessed as per the completeness of answering the following questions:

- *19.1.1 Security Organization and Program Governance*
    - Has a DSO been appointed? If a DSO has not been appointed (or is under acting assignment), are there plans to permanently staff the position before the end of this Fiscal Year?
    - Is the DSO strategically positioned within the organization, to provide department- or agency-wide advice and guidance to senior management?
    - Is there a security organization with established governance (e.g. senior management committees, working groups), key security positions (i.e. DSO, IT Security Manager/Coordinator and BCP Manager/Coordinators/Planners), roles and responsibilities, and coordination mechanisms to ensure effective management of the departmental security program? Where responsibilities are delegated to another organization, are mechanisms establishing respective responsibilities and accountabilities of stakeholders in place (e.g. MOU that clearly details roles and responsibilities of participants)?
    - Is there a security program, with established strategies, work plans, policies, procedures, and practices that ensure coordination of key security policy functions (i.e. personnel screening, physical security, IT security, security in contracting and BCP) and implementation of related policy requirements?

- *19.1.2 Sharing of information and assets*
    - Are measures in place to ensure that agreements are established when sharing information or assets with organizations outside the federal government (outside of a contractual context), and that these agreements specify security responsibilities, safeguards to be applied, and terms and conditions for continued participation?
    - Is there evidence that sharing agreements are in place (based on departmental requirements), include appropriate security provisions, are being monitored on an on-going basis to verify compliance with security provisions, and are periodically reviewed to confirm their status and relevance?

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

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

- *19.1.5 Security briefings*
    - 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) and that they sign the appropriate briefing forms?

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

Additionally, to obtain a Strong rating, departments and agencies need to demonstrate leadership and contribute to the government-wide security program. Furthermore, the organization's security strategy needs to be aligned and integrated with its corporate priorities and business plan.

3. **Rating:**

The Departmental Security Program line of evidence (LoE) will be rated according to the following scale:

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.

Line of Evidence 19.2: Management of Information Technology Security

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

1. **Evidence: Completed MITS questionnaire**

The MITS self-assessment questionnaire was developed by the Secretariat to analyze and monitor departmental and government-wide compliance with the MITS standard. The questionnaire assesses compliance with all MITS requirements in addition to the three priority objectives. For MAF Round VI, departments and agencies are required to submit a completed questionnaire that reflects their current state of compliance with MITS and anticipated progress until the end of February 2009. Departments and agencies that were assessed in Round V need to provide an update of the MITS assessment submitted in that round, to reflect progress made in the last year with regards to previously identified areas of deficiency or to revise responses in areas where they may no longer be compliant due to changes in the organization or their practices.

Notes:

- *The overview document needs to indicate the date of the MITS questionnaire submitted that is to be used for the Round VI assessments. If an update to the MITS questionnaire is submitted **during** the MAF Round VI assessment period, the overview document also needs to be updated accordingly.*
- *In preparing their MAF Round VI submission, departments and agencies should review the results of internal audits, evaluations, and other sources (including independent assessments, recent incident reports, MAF Round V assessments if available, and MAF Round VI submission as it pertains to the departmental security and BCP programs) to validate the accuracy of their MITS self-assessment. The Secretariat may use these other sources to validate departmental MITS self-assessments and may request clarification from departments and agencies where discrepancies are identified.*

2. **Analytical approach:**

Evaluations will be based on the compliance with the following three priority objectives and key MITS requirements, as reported by departments and agencies in the MITS questionnaire:

- *Priority objectives:*
    - Departments and agencies have IT security fundamentals in place, including appropriate people, processes and strategies, an effective IT security organization, and a risk management program
    - Departments and agencies have identified their critical systems and taken action to ensure they are secure
    - Departmental senior management understands the potential impact of IT security risks within the context of the overall departmental risk profile and has assigned appropriate priority to addressing those risks

- MITS *requirements*
    - IT security organization
    - IT security policy
    - IT security resources and system development life cycle
    - Identification of assets
    - Risk management
    - Incident management
    - Vulnerability management
    - Continuity planning
    - Audit, monitoring and assessment

- Awareness
- Other technical and operational safeguards

Additionally, to obtain a Strong rating, departments and agencies need to demonstrate leadership and contribute to the government-wide IT security program.

3. **Rating:**

The MITS line of evidence will be rated according to the following scale:

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.

Line of Evidence 19.3: Business Continuity Planning 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.

1. **Evidence: Completed BCP Program Compliance Report**

The BCP Program Compliance Report (formerly known as the BCP Action Plan Template) was developed by Public Safety Canada to facilitate its assessment of departmental compliance with the BCP Program standard. The report template still consists of four score cards, one for each element of the BCP life cycle outlined in the standard. Each element is divided into subgroups of metrics and associated best practices. The report is used by departments and agencies for self assessment and submitted to Public Safety Canada who will compile, analyze, and validate the results.

Public Safety Canada will assist all departments and agencies that are assessed in Round VI with the completion of their self-assessments using the compliance report template. The results will also be provided to the Secretariat and will form the basis of the MAF assessment for this line of evidence.

Departments and agencies are **not** required to provide any additional evidence to substantiate the assertions contained in their completed BCP Program Compliance Report. Public Safety Canada and the Secretariat may use other sources such as departmental internal audit results to validate the BCP Program Compliance Report, and may request clarification from departments and agencies where discrepancies are identified.

Notes:

*The overview document needs to indicate the last update of the BCP Program Compliance Report submitted to Public Safety Canada and that is to be used for the Round VI assessments. If an update to the BCP Program Compliance Report is submitted **during** the MAF Round VI assessment period, the overview document also needs to be updated accordingly.*

2. **Analytical approach:**

Evaluations will be based on the extent to which the department or agency has complied with the BCP Program standard requirements, which includes:

- *BCP Program Governance:* A governance structure that establishes authorities and responsibilities for the BCP program, and for the development and approval of business continuity plans is in place
- *Business Impact Analysis (BIA):* A BIA has been conducted to identify and prioritize the department or agency's critical services and assets, and the BIA results have been approved by senior management
- *BCP Plans and Arrangements:* business continuity plans, contingency plans, measures and arrangements are in place to ensure the continued availability of critical business services/functions and assets and of any other service or asset when warranted by a threat and risk assessment
- *BCP Readiness:* Activities are conducted to monitor the department's (or agency's) level of overall readiness and to provide for the continuous review, exercising, testing, and audit of business continuity plans

Additionally, to obtain a Strong rating, departments and agencies need to have approved readiness plans in place for pandemic and information management/information technology (IM/IT) emergency preparedness.

3. **Rating:**

The BCP program line of evidence will be rated according to the following scale:

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.

IV—EVIDENCE CHECK LISTS

This section provides a summary of the evidence requirements for Area of Management 19 and for each line of evidence, as further detailed in section III.

Area of Management 19: Security and Business Continuity

- ☐ Overview document (prepared using response template), which includes:
  - Document inventory (listing all documents submitted for 19.1)
  - Part A—Description of security activities, policy compliance and management performance for each assessment element, with references to the applicable documents submitted as evidence (for 19.1)
  - Part B—Identification of date of questionnaires submitted and related information for 19.2 and 19.3
  - Part C—Information related to elements assessed for Strong rating (for 19.1 and 19.2):
    - Leadership and extra-organizational contributions
    - Strategic alignment
  - Part D—Description of performance measurement, internal audits, management reviews, evaluations and other assessments of security program (for 19.1, 19.2 and 19.3)
  - Part E—Additional information (optional – may include description of significant barriers to progress or suggestions on how to improve the MAF assessment process for this area of management)

Line of Evidence 19.1: Departmental Security Program

- ☐ Evidence related to Security Organization and Program Governance:
  - DSO appointment—DSO title, classification, and appointment status (staffing plans if applicable)
  - DSO strategic positioning—Reporting relationship between DSO and departmental executive, and mechanisms used to engage and advise senior management
  - Security organization and governance—Description of departmental security organization, reporting relationships, governance structure, coordination mechanisms, and resources allocation (FTEs, salary budget and classification)
    - ***Note:*** *Evidence need to include governance and coordination mechanisms when security services are provided by third party.*
  - Departmental security program—Departmental security strategies, policies, and work plans addressing key policy functions
    - ***Note:*** *When security policies from another organization are used, evidence is needed of decision to adopt these policies and any adaptation to them.*
- ☐ Departmental policy requirements, roles and responsibilities, and practices and procedures related to the following assessment elements:
  - Sharing of information and assets
  - Security training
  - Security awareness
  - Security briefings
  - Incident management

Line of Evidence 19.2: Management of Information Technology Security

- ☐ MITS questionnaire

Line of Evidence 19.3: Business Continuity Planning Program

- ☐ BCP Program Compliance Report (submitted directly to Public Safety Canada)