AoM 19 - Security and Business Continuity

Ratings Descriptions - English

	Attention Required	Opportunity for Improvement	Acceptable	Strong
Area of Management	Fundamental security management practices are not in place, risks to the organization's resources and operations are not understood and there is no apparent senior management engagement in the management of security risks. As a consequence, information and other resources are likely exposed and at risk, and/or the organization's ability to maintain critical services and business operations is unknown and would likely be very limited.	Although some security management practices are in place, significant deficiencies have been identified in meeting key policy requirements. It appears that senior management is not fully engaged in the management of security risks. As a consequence, the organization has only a limited capability to safeguard information, and other resources, and/or their ability to maintain critical services and business operations cannot be assured.	Fundamental security management practices are in place, risks to the organization's resources and operations are well understood and senior management is engaged in the management of security risks. As a consequence, the organization has safeguards in place that will likely assure the security of its information and other resources, and continued availability of its critical services and business operations.	With the continuous engagement and oversight of senior management, the organization sustains and continually strengthens its management of security risks and readiness to continue critical business operations. The organization meets most or all security policy requirements, and can provide a high degree of assurance of its security and continued availability of critical services and business operations.
19.1 Departmental Security Program (DSP)	The organization has limited or no evidence of leadership, administration, or implementation of a security program that includes key policy elements. There are several significant deficiencies in meeting key policy requirements for the departmental security	The organization has a partially developed security program that contains some of the required policy elements. Significant Deficiencies remain in meeting key policy requirements for the departmental security	The organization has in place a fully developed security program that comprises key policy elements and is administered by an appointed Departmental Security Officer (DSO) who is positioned to	The organization's security program is fully developed and sustainable, and comprises all key policy elements. The organization demonstrates leadership and contributes to the government-wide

	program.	program.	provide strategic advice and guidance to senior management. No significant deficiencies remain in meeting key policy requirements for the departmental security program.	security program, and its security strategy is completely aligned and integrated with its corporate priorities and business plan.
19.2 Management of Information Technology Security (MITS)	The organization has not achieved the three priority objectives that form the foundation for Management of Information Technology Security (MITS) and include having IT security fundamentals in place, securing critical systems, and prioritizing IT security risks within the context of overall organizational risks.	The organization has achieved the three priority objectives that form the foundation for Management of Information Technology Security (MITS), but does not fully comply with MITS requirements. Significant deficiencies remain in meeting key MITS requirements.	The organization has achieved the three priority objectives that form the foundation for Management of Information Technology Security (MITS) and complies with most MITS requirements. No significant deficiencies remain in meeting key MITS requirements.	The organization fully complies with Management of Information Technology Security (MITS) requirements, demonstrates leadership and contributes to the government-wide Information Technology security program.
19.3 Business Continuity Planning (BCP) Program	The organization does not have measures in place to provide for the continuity of critical business operations and services.	The organization has partially developed measures to provide for the continuity of critical business operations and services.	The organization has in place measures to provide for the continuity of critical business operations and services, and is compliant with most or all the policy requirements.	The organization has a fully developed and sustainable ability to provide for the continuity of critical business operations and services. Completed and approved plans are in place for Pandemic and Information Management / Information Technology emergency preparedness.

Ratings Descriptions - French

	Attention Requise	Possibilité d'amélioration	Acceptable	Fort
Composante de gestion	Les pratiques de base en matière de gestion de la sécurité ne sont pas en place, les risques visant les ressources et les opérations de l'organisation ne sont pas bien compris et il n'y a pas d'engagement apparent de la haute direction dans la gestion des risques relatifs à la sécurité. Par conséquent, l'information et autres ressources sont susceptibles d'être exposés et sont potentiellement à risque, et/ou la capacité de l'organisation de maintenir les services et activités essentiels est inconnue et serait vraisemblablement limitée.	Bien que les certaines pratiques en matière de gestion de la sécurité sont en place, des lacunes importantes existent au plan des exigences clés de politique. Il semble que la haute direction ne soit pas pleinement engagée à l'égard de la gestion des risques relatifs à la sécurité. Par conséquent, l'organisation a seulement une capacité limitée de protéger son information et ses autres ressources, et/ou de maintenir les services et activités essentiels.	Les pratiques de base en matière de gestion de la sécurité sont en place, les risques visant les ressources et les opérations de l'organisation sont bien compris et la haute direction est engagée dans la gestion des risques relatifs à la sécurité. Par conséquent, l'organisation a les mesures de protection nécessaires en place pour assurer, selon toute vraisemblance, la sécurité de son information et ses autres ressources, et l'accès continu à ses services et activités essentiels.	Grâce à l'engagement et à la supervision continus de la haute direction, l'organisation soutient et consolide continuellement sa gestion des risques relatifs à la sécurité et son état de préparation pour assurer la continuité des activités essentielles. L'organisation rencontre la plupart ou toutes les exigences de politique en matière de sécurité, et peut fournir un niveau supérieur d'assurance à l'égard de sa sécurité et du maintien de la continuité des services et activités essentiels.
19.1 Programme de sécurité ministériel (PSM)	L'organisation a fourni une preuve limitée ou inexistante à l'égard d'un leadership, de l'administration ou de la mise en œuvre d'un programme de sécurité comprenant les principaux éléments de la politique. Plusieurs lacunes notables demeurent en ce qui a	L'organisation est dotée d'un programme de sécurité partiellement développé comprenant certains des éléments de la politique requis. Des lacunes notables demeurent en ce qui a trait à la conformité aux	L'organisation est dotée d'un programme de sécurité complet comprenant les principaux éléments de la politique et qui est administré par un Agent de sécurité ministériel (ASM) positionné de	Le programme de sécurité de l'organisation est complet, durable et comprend tous les éléments clés de la politique. L'organisation fait preuve de leadership et contribue au programme de sécurité à l'échelle du gouvernement, et sa stratégie de sécurité est

	trait à la conformité aux éléments clés de la politique en matière de programme de sécurité.	éléments clés de la politique en matière de programme de sécurité.	façon à pouvoir fournir des conseils et des orientations stratégiques à la haute direction. Aucunes lacunes notables ne demeurent en ce qui a trait à la conformité aux éléments clés de la politique en matière de programme de sécurité.	harmonisée et intégrée avec ses priorités et son plan d'activité ministériels.
19.2 Gestion de la sécurité des technologies de l'information (GSTI)	L'organisation n'a pas réalisé les trois objectifs prioritaires qui forment la base de la Gestion de la sécurité des technologies de l'information (GSTI) et comprennent les éléments fondamentaux de sécurité des technologies de l'information (TI), la protection des systèmes essentiels et l'établissement de l'ordre de priorité des risques à la sécurité des TI dans le contexte des risques globaux de l'organisation.	L'organisation a réalisé les trois objectifs prioritaires qui forment la base de la Gestion de la sécurité des technologies de l'information (GSTI) mais ne s'est pas entièrement conformée aux exigences de la GSTI. Des lacunes notables demeurent au plan des exigences clés de la GSTI.	L'organisation a réalisé les trois objectifs prioritaires en matière de Gestion de la sécurité des technologies de l'information (GSTI) et se conforme à la plupart des exigences de la GSTI. Aucunes lacunes notables au plan des exigences clés de la GSTI.	L'organisation se conforme entièrement aux exigences de politique en matière de gestion de la sécurité des technologies de l'information (GSTI), fait preuve de leadership et contribue au programme de sécurité des technologies de l'information à l'échelle du gouvernement.
19.3 Planification de la continuité des activités (PCA)	L'organisation n'a pas mis en place des mesures permettant d'assurer la continuité des activités et services essentiels.	L'organisation a mis en place des mesures incomplètes pour assurer la continuité des activités et services essentiels.	L'organisation a en place des mesures permettant d'assurer la continuité des activités et services essentiels et se conforme à la plupart ou toutes les exigences de la politique.	L'organisation a une capacité complète et durable d'assurer la continuité des activités et services essentiels. Les plans d'intervention sont terminés et approuvés pour les mesures d'urgence en cas de pandémie et de problème de gestion de l'information / gestion des technologies de l'information.