BSIF B-13 : grille d'autoévaluation

Groupe Conseil GRD. Source officielle : BSIF, ligne directrice B-13, Gestion du risque lié aux technologies et du cyberrisque (en vigueur le 1er janvier 2024). FR : https://www.osfi-bsif.gc.ca/fr/consignes/repertoire-consignes/gestion-du-risque-lie-technologies-du-cyberrisque ; EN : https://www.osfi-bsif.gc.ca/en/guidance/guidance-library/technology-cyber-risk-management

Mode d'emploi : pour chaque attente, cochez Conforme, Partiel ou Non conforme et indiquez la preuve (document, rapport, capture). Les énoncés ci-dessous résument les attentes de B-13 avec leur numéro de section ; le texte officiel du BSIF fait foi. La colonne « Outils Microsoft utiles » est une suggestion de Groupe Conseil GRD, pas une exigence du BSIF.

Domaine 1. Gouvernance et gestion du risque

Résultat attendu : les risques technologiques et cyber sont encadrés par des responsabilités et structures claires, et par des stratégies et cadres complets. Outils Microsoft utiles : Secure Score, MCSB.

Section	Attente B-13	Conforme	Partiel	Non conforme	Preuve
1.1.1	La haute direction confie la responsabilité de la gouvernance des risques technologiques et cyber à des cadres supérieurs (ex. CTO, CIO, CISO) ayant l'envergure et la visibilité voulues.	☐	☐	☐	
1.1.2	Une structure organisationnelle avec rôles clairs, ressources humaines et financières suffisantes, expertise et formation est en place; la haute direction compte des personnes qui comprennent ces risques; une culture de sensibilisation au risque est promue.	☐	☐	☐	
1.2.1	Un plan stratégique technologique et cyber est défini, documenté, approuvé et mis en œuvre : il anticipe les changements, mentionne les changements prévus, précise moteurs, occasions, vulnérabilités, menaces et mesures de suivi, inclut des indicateurs de risque et explique son appui à la stratégie d'affaires.	☐	☐	☐	
1.3.1	Un cadre de gestion des risques technologiques et cyber (CGR) est aligné sur le cadre de gestion des risques d'entreprise et revu régulièrement à partir des leçons apprises (ex. incidents passés).	☐	☐	☐	
1.3.2	Le CGR couvre : responsabilités (y compris fonctions de surveillance), appétit pour le risque et mesures (limites, seuils, tolérances), taxonomie des risques, domaines de contrôle, politiques et normes approuvées et revues, processus d'identification à la déclaration (y compris exceptions), risques des menaces et technologies émergentes, rapports à la haute direction.	☐	☐	☐	

Domaine 2. Activités et résilience technologiques

Résultat attendu : un environnement technologique stable, évolutif et résilient, maintenu à jour et soutenu par des processus d'exploitation et de reprise robustes. Outils Microsoft utiles : Defender for Cloud, comptes d'accès d'urgence.

Section	Attente B-13	Conforme	Partiel	Non conforme	Preuve
2.1.1	Un cadre de principes d'architecture TI encadre l'architecture dans toute l'institution, en appui aux objectifs technologiques, de sécurité et d'affaires.	☐	☐	☐	
2.1.2	L'architecture est complète (infrastructure, applications, technologies émergentes, données) et les systèmes visent disponibilité, évolutivité, sécurité dès la conception et résilience dès la conception, selon une approche fondée sur le risque.	☐	☐	☐	
2.2.1	Des normes et procédures de gestion des actifs technologiques sont établies.	☐	☐	☐	
2.2.2	Un inventaire à jour et complet des actifs est tenu sur tout leur cycle de vie, avec catégorisation selon la criticité ou la classification et documentation des interdépendances entre actifs critiques.	☐	☐	☐	
2.2.3	L'inventaire consigne et gère les configurations; les écarts par rapport à la configuration de référence approuvée sont repérés, évalués, corrigés et signalés.	☐	☐	☐	
2.2.4	Des normes et processus assurent l'élimination ou la destruction sécuritaire des actifs.	☐	☐	☐	
2.2.5	La mise à niveau (« currency ») des logiciels et du matériel est surveillée en continu; les actifs non corrigés, désuets ou non soutenus sont gérés et remplacés avant la fin du soutien.	☐	☐	☐	
2.3.1	Les projets technologiques sont régis par un cadre de gestion de projets à l'échelle de l'entreprise; leur performance et leurs risques sont mesurés, suivis et déclarés périodiquement.	☐	☐	☐	
2.4.1	Un cadre de cycle de développement des systèmes (SDLC) définit processus et contrôles à chaque phase pour la sécurité et la fonctionnalité.	☐	☐	☐	
2.4.2	Des points de contrôle intègrent les exigences de sécurité à chaque phase du SDLC, y compris en mode Agile.	☐	☐	☐	
2.4.3	Les pratiques intégrant développement, sécurité et exploitation (DevSecOps) sont alignées sur le cadre SDLC et les politiques applicables.	☐	☐	☐	
2.4.4	Les systèmes et logiciels acquis font l'objet d'évaluations des risques de sécurité et des contrôles du SDLC.	☐	☐	☐	
2.4.5	Des principes et bonnes pratiques de codage sont définis et appliqués (codage sécuritaire, code tiers et libre, dépôts et outils).	☐	☐	☐	
2.5.1	Les changements en production sont documentés, évalués, testés, approuvés, mis en œuvre et vérifiés de façon contrôlée, y compris les changements d'urgence.	☐	☐	☐	
2.5.2	La séparation des tâches empêche une même personne de développer, autoriser, exécuter et déplacer du code entre environnements de production et hors production.	☐	☐	☐	
2.5.3	La traçabilité et l'intégrité des dossiers de changement et des actifs modifiés sont assurées à chaque phase.	☐	☐	☐	
2.6.1	Les correctifs sont appliqués en temps opportun et de façon contrôlée : rôles définis, processus de gestion des changements suivi, tests avant la production.	☐	☐	☐	

Section	Attente B-13	Conforme	Partiel	Non conforme	Preuve
2.7.1	Des normes et processus de gestion des incidents et des problèmes assurent détection et escalade rapides, rétablissement et analyse des causes.	☐	☐	☐	
2.7.2	Le processus d'incident prévoit notamment : rôles internes et externes, indicateurs d'alerte précoce, classification selon l'impact, procédures de réponse et de communication, tests et exercices périodiques, y compris avec les tiers.	☐	☐	☐	
2.7.3	La gestion des problèmes inclut revues post-incident, analyse des causes et des tendances, et sert à améliorer les processus (y compris changements et mises en production).	☐	☐	☐	
2.8.1	Des normes de gestion des services TI avec indicateurs ou cibles mesurent la prestation, avec correctifs lorsque les cibles ne sont pas atteintes.	☐	☐	☐	
2.8.2	Des exigences de performance et de capacité avec seuils d'utilisation sont définies et surveillées en continu.	☐	☐	☐	
2.9.1	Un programme de reprise après sinistre d'entreprise (EDRP), aligné sur la continuité des affaires, établit responsabilités, analyse des services et dépendances, plans de reprise dans des délais acceptables et une politique de sauvegarde, de stockage et de tests.	☐	☐	☐	
2.9.2	Les dépendances clés du EDRP sont gérées : exigences de sécurité des données (ex. chiffrement) et emplacement des centres, sites de relève et fournisseurs.	☐	☐	☐	
2.9.3	Les capacités de reprise sont testées régulièrement selon des scénarios graves mais plausibles, y compris sauvegardes, récupération et technologies tierces critiques, et les résultats sont déclarés.	☐	☐	☐	

Domaine 3. Cybersécurité

Résultat attendu : une posture de sécurité qui maintient la confidentialité, l'intégrité et la disponibilité des actifs technologiques. Outils Microsoft utiles : authentification multifacteur, PIM, journal d'audit.

Section	Attente B-13	Conforme	Partiel	Non conforme	Preuve
3.0	Les menaces, événements et incidents externes et internes sont identifiés, contrés, détectés, traités et suivis d'un rétablissement de façon proactive.	☐	☐	☐	
3.1.1	Les cybermenaces actuelles et émergentes sont repérées par des évaluations des menaces et des risques couvrant plusieurs couches de défense.	☐	☐	☐	
3.1.2	Des évaluations et tests guidés par le renseignement (ex. tests d'intrusion, red teaming) ont des déclencheurs et fréquences minimales définis et une portée encadrée.	☐	☐	☐	
3.1.3	Des évaluations de vulnérabilités régulières, à fréquence définie, classent les vulnérabilités selon une méthode standard, en tenant compte de leur effet cumulatif.	☐	☐	☐	

Section	Attente B-13	Conforme	Partiel	Non conforme	Preuve
3.1.4	Les données structurées et non structurées sont repérées, classifiées et protégées; des balayages périodiques détectent les écarts.	☐	☐	☐	
3.1.5	Une connaissance continue de la situation des menaces est maintenue (ex. forums de partage, sources de renseignement fiables).	☐	☐	☐	
3.1.6	Lorsque possible, des modèles de menaces sont tenus et une chasse aux menaces manuelle complète les outils automatisés.	☐	☐	☐	
3.1.7	Employés, clients et tiers sont encouragés à signaler les activités suspectes; la sensibilisation est faite et testée régulièrement.	☐	☐	☐	
3.1.8	Un profil de cyberrisque à jour est tenu et déclaré; les risques résiduels sont mesurés, suivis et agrégés.	☐	☐	☐	
3.2.1	Des pratiques de sécurité dès la conception sont adoptées, avec priorité aux contrôles préventifs, y compris pour les applications, microservices et API.	☐	☐	☐	
3.2.2	Des technologies cryptographiques robustes protègent les actifs; les clés sont protégées tout au long de leur cycle de vie; la norme de cryptographie est réévaluée régulièrement.	☐	☐	☐	
3.2.3	Des contrôles renforcés protègent les actifs critiques et exposés à l'externe : contrôles requis définis, limitation de l'impact, normes et configurations de durcissement, couches supplémentaires (ex. attaques volumétriques).	☐	☐	☐	
3.2.4	Les contrôles sont en couches à chaque étape du cycle d'attaque : réduction de la surface d'attaque, zones réseau segmentées, listes d'autorisation et de refus, prévention et détection d'intrusion, contrôles anti-perte de données et anti-maliciel.	☐	☐	☐	
3.2.5	Selon la classification de l'information, des contrôles de protection et de prévention de la perte de données couvrent les données au repos, en transit et en cours d'utilisation.	☐	☐	☐	
3.2.6	Les vulnérabilités sont corrigées selon le risque et des délais établis, avec mesures compensatoires au besoin (ex. « jour zéro ») et suivi de l'état, des retards et des exceptions.	☐	☐	☐	
3.2.7	Des contrôles d'identité et d'accès fondés sur le risque sont en place : moindre privilège, attestations d'accès régulières, authentification multifacteur sur les canaux externes et comptes privilégiés, coffre pour les identifiants privilégiés, journalisation des comptes, comptes de service surveillés, vérifications d'antécédents lorsque possible.	☐	☐	☐	
3.2.8	Des configurations de sécurité de référence approuvées s'appliquent aux actifs et outils (y compris ceux de tiers), désactivant par défaut lorsque possible; les écarts sont gérés.	☐	☐	☐	
3.2.9	Lorsque possible, des analyses statiques ou dynamiques évaluent les systèmes nouveaux ou modifiés avant la production, y compris dans les chaînes de déploiement automatisées.	☐	☐	☐	

Section	Attente B-13	Conforme	Partiel	Non conforme	Preuve
3.2.10	Des contrôles d'accès physique protègent l'infrastructure réseau et les actifs contre les accès non autorisés et les risques environnementaux.	☐	☐	☐	
3.3.1	La journalisation de sécurité est continue et centralisée, avec durées minimales de conservation permettant une enquête judiciaire complète.	☐	☐	☐	
3.3.2	Des capacités SIEM détectent et signalent en continu les activités malveillantes ou non autorisées, avec détection comportementale lorsque possible et indicateurs de compromission à jour.	☐	☐	☐	
3.3.3	Des rôles sont définis pour trier rapidement les alertes à risque élevé.	☐	☐	☐	
3.4.1	Les capacités de réponse cyber sont intégrées aux protocoles technologiques, de gestion de crise et de communication, avec escalade et coordination des parties prenantes.	☐	☐	☐	
3.4.2	Une taxonomie des cyberincidents (gravité, catégorie, type, cause) est définie et appliquée.	☐	☐	☐	
3.4.3	Un processus de gestion des cyberincidents et des guides d'intervention (playbooks) sont tenus à jour.	☐	☐	☐	
3.4.4	Une équipe d'intervention disponible en continu peut répondre, contenir et rétablir rapidement.	☐	☐	☐	
3.4.5	Une enquête judiciaire est menée lorsque des actifs ont pu être exposés; pour les incidents graves, une évaluation post-incident et une analyse des causes couvrent personnes, processus, technologie et données.	☐	☐	☐	

Le BSIF publie aussi un outil d'autoévaluation officiel (Technology and cyber risk management self-assessment tool) lié à la page de B-13.

Besoin d'aide pour votre autoévaluation ? Demander une soumission : info@grdinc.ca, 514 291-9003.