|  |  |
| --- | --- |
| **Conseil 2020Genève, 9-19 juin 2020** |  |
|  |  |
|  |  |
| **Point de l'ordre du jour: ADM 6** | **Document C20/15-F** |
| **30 mars 2020** |
| **Original: anglais** |
| Rapport du Secrétaire général |
| système de gestion de la résilience de L'organisation (ORMS) |

|  |
| --- |
| RésuméÀ sa session de 2017, le Conseil a approuvé la mise en place d'un projet de système de gestion de la résilience de l'organisation (ORMS).On trouvera dans le présent rapport des informations générales sur le projet, un résumé des conclusions du projet comprenant une description du cadre ORMS (continuité des activités (BC) et gestion des crises (CM)) et trois recommandations.Suite à donnerLe Conseil est invité à **prendre note** du présent rapport, à **approuver** les recommandations et à **formuler des avis** concernant les possibles sources de financement d'un projet de classification des données.\_\_\_\_\_\_\_\_\_\_\_\_Références[C16/70](https://www.itu.int/md/S16-CL-C-0070/en), [C17/63](https://www.itu.int/md/S17-CL-C-0063/en), [C20/53](https://www.itu.int/md/S20-CL-C-0053/en) |

Aperçu et résultats du projet ORMS

# 1 Rappel

La politique relative au système de gestion de la résilience des organisations (ORMS) appartenant au système des Nations Unies a été approuvée par le Conseil des chefs de Secrétariat (CCS) des Nations Unies en 2014 et adoptée par le Conseil de l'UIT en 2016 (Document C16/70).

À sa session de 2017, le Conseil a approuvé le projet ORMS de l'UIT, car depuis sa création en 1865, l'Union s'était dotée de plans en cas d'urgence liée à la sécurité, mais jamais de plans de gestion des crises ou de continuité des activités. Le projet a débuté le 1er novembre 2017 et s'est achevé le 31 décembre 2019, dans les délais et le budget fixés. Deux consultants ont été recrutés pour ce projet et ont effectué le travail suivant: recherche, entretiens (plusieurs centaines), visite dans tous les bureaux hors siège de l'UIT, organisation de séances d'information à l'intention des fonctionnaires, organisation de deux exercices théoriques de gestion de crise et élaboration de plus de 40 rapports. Tous les fonctionnaires élus de l'UIT, les responsables, les fonctionnaires des bureaux régionaux et des bureaux de zone ainsi que de nombreux autres collègues, y compris des institutions, fonds et programmes des Nations Unies à Genève et à New York, ont été associés à ce travail. En outre, des rencontres ont eu lieu avec des responsables des Nations Unies et des fonctionnaires du Département de la sûreté et de la sécurité des Nations Unies dans les douze pays où l'UIT a des bureaux hors siège, afin de s'assurer que les fonctionnaires de l'Union sont couverts de manière satisfaisante par le système de gestion de la sécurité des Nations Unies dans ces pays.

À sa session de 2017, le Conseil a en outre approuvé la création d'un poste P4 à compter de 2020, pour coordonner et gérer les tâches de maintenance, de simulation et d'examen du système ORMS; au moment où nous rédigeons le présent document, la procédure de recrutement est en cours.

# 2 Cadre ORMS de l'UIT

Le cadre ORMS comprend sept éléments peut être divisé en deux composantes: continuité des activités (BC) et gestion des crises (CM).

## 2.1 Continuité des activités

La continuité des activités (BC) est la capacité de l'organisation de continuer de fournir des produits ou des services selon des niveaux acceptables prédéfinis après un événement perturbateur.

Le système de gestion de la continuité des activités (BCMS), élaboré compte tenu des normes et bonnes pratiques internationales actuelles, est composé d'un groupe structuré de documents comprenant une politique, des plans, des lignes directrices et des rapports qui, ensemble, permettent d'assurer la continuité des activités. Il se présente en quatre sections − préparation, amélioration, mise en œuvre et examen − et fait l'objet de l'Annexe 1.

## 2.2 Gestion des crises

Une approche globale a été mise en place pour la gestion efficace des crises pour toutes les activités de l'UIT partout dans le monde.

Dans le contexte de la responsabilité principale qui incombe à un pays hôte et au système de gestion de la sécurité des Nations Unies (UNSMS) et comprend la gestion globale des crises liées à la sécurité, l'UIT est désormais dotée d'une capacité institutionnelle et développe des capacités de gestion des crises, que l'incident grave à l'origine de la crise se produise au siège, dans un bureau régional ou dans un bureau de zone, ou qu'il concerne plusieurs ou tous les bureaux de l'UIT.

Il existe désormais une structure CM fondée sur un cadre institutionnel de responsabilité pour la sécurité et composée d'une politique, de lignes directrices et de procédures, et avec une répartition définie des responsabilités et rôles clés. Cette structure est conçue de manière à être souple et utilisable quel que soit l'incident grave ou l'urgence, y compris en cas de perturbation importante des activités, susceptible d'aboutir à une crise.

En effet, il a été démontré que des connaissances avaient été acquises concernant la gestion des crises et la continuité des activités lors de deux incidents différents pour lesquels l'Équipe de gestion des crises (CMT) de l'UIT a été activée, la première fois en mars 2019 lorsque l'Équipe CMT a été convoquée sur le plan opérationnel lors du tragique accident dont a été victime le vol ET-302 en Éthiopie, dans lequel deux fonctionnaires du Bureau régional pour l'Afrique ont perdu la vie, et la seconde fois en février 2020, pour faire face à la flambée de Covid-19 et à la pandémie qui a suivi, laquelle est toujours en cours au moment où nous rédigeons le présent document.

On trouvera dans l'Annexe 2 les composantes et des informations détaillées sur cette structure de gestion des crises.

# 3 Indicateurs de résultats des Nations Unies/de l'UIT

Outre la politique ORMS du système des Nations Unies, le CCS a également approuvé un dispositif de maintenance, de simulation et d'examen (MER) du système ORMS, ainsi que des indicateurs de résultats. Le dispositif MER comprend les éléments suivants: formation et sensibilisation, responsabilités décisionnelles, réponse en cas de crise, communication, continuité des activités, rétablissement TIC après une catastrophe, analyse a posteriori, tests et mise à jour et approbation.

Le dispositif MER a été intégré à ce projet, comme l'a recommandé le Conseil à sa session de 2016, qui a également recommandé que l'UIT adopte les indicateurs de résultats associés au système ORMS des Nations Unies.

# 4 Gestion des risques liés aux activités

**Il est reconnu qu'un effet négatif sur la réputation de l'UIT est un risque important pour l'organisation. On estime que la consolidation d'un processus efficace d'évaluation et de gestion des risques opérationnels pour les activités est une priorité**, compte tenu des propositions et lignes directrices émanant de l'Équipe spéciale multifonctionnelle du CCS sur la gestion des risques et du fait que Comité consultatif pour les questions administratives et budgétaires (CCQAB) a reconnu la nécessité de consolider "*...les meilleures pratiques et données d’expérience en matière de gestion des risques et de gestion de la résilience organisationnelle...*", il est recommandé d'adopter un mécanisme unique de gestion des risques et de l'adapter afin de couvrir l'analyse, l'appréciation et la prise de décisions concernant la gestion à la fois des risques liés à la sécurité et des risques liés aux activités; il est en outre recommandé de créer un poste de responsable de la gestion des risques liés aux activités pour l'organisation, dont le titulaire travaillera en étroite collaboration avec le coordonnateur ORMS et le responsable TIC de la continuité des activités/du rétablissement après une catastrophe, sous la supervision du Chef de la Division de la sûreté et de la sécurité (SSD) qui est chargé de la gestion des risques liés à la sécurité au sein de l'Union.

# 5 Classification des données en fonction de la sensibilité et de la criticité

Il existe un risque organisationnel important découlant des cyberattaques et des dénis de service, qui pourrait avoir des incidences sur les données fournies à l'UIT par les États Membres. Selon les conclusions du projet ORMS, l'UIT a besoin d'un système de classification des données permettant de déterminer leur "sensibilité et criticité", afin de prévenir et de maîtriser ce risque. Cette élément est conforme et fait suite à l'évaluation des risques transitoires liés au nouveau bâtiment, qui a mis en évidence la nécessité de répertorier et d'indexer les exemplaires physiques des documents actuellement conservés par le Bureau des radiocommunications (BR) pour rendre possible la continuité des activités – exigence que le Conseil, à sa session de 2019, a approuvée et financée.

# 6 Examen de la résilience des fonctionnaires des ressources humaines

L'évaluation des risques liés aux activités a montré un manque de résilience des ressources humaines de l'organisation. En particulier, le manque de planification du renouvellement des effectifs et la perte des connaissances institutionnelles et techniques découlant du remplacement différé de fonctionnaires occupant des fonctions et des rôles clés pourraient constituer un risque grave pour la réputation de l'UIT.

# 7 Recommandations

Les résultats attendus du projet ORMS ont été obtenus et les conclusions formulées à l'issue du projet ont abouti aux recommandations suivantes:

1) Adoption d'un mécanisme unique de gestion des risques couvrant l'analyse, l'appréciation et la prise de décisions concernant la gestion à la fois des risques liés à la sécurité et des risques liés aux activités.

2) Création d'un poste de responsable de la gestion des risques liés aux activités de l'organisation, dans les limites du budget disponible, qui travaillera en collaboration étroite avec le coordonnateur ORMS et le responsable TIC de la continuité des activités/du rétablissement après une catastrophe, sous la supervision du Chef de la Division de la sûreté et de la sécurité (SSD) qui est chargé de la gestion des risques liés à la sécurité au sein de l'Union.

3) Création d'un projet visant à définir un système de classification des données à l'UIT et à l'appliquer aux nouvelles données reçues.

Il est demandé au Conseil de formuler des avis concernant les sources possibles de financement du projet de classification des données susmentionné.

ANNEXE 1

Continuité des activités

La continuité des activités (BC) se présente en quatre sections, à savoir préparation, amélioration, mise en œuvre et examen, comme suit:

# 1 Préparation

Politique de continuité des activités (politique BC)

La politique BC a été élaborée lors du projet ORMS. Son objectif est de garantir qu'après un événement perturbateur, l'organisation est capable de fournir des activités définies comme étant prioritaires à des niveaux acceptables déterminés au préalable. Cette politique s'applique à l'ensemble des fonctionnaires, des locaux et des équipements de l'organisation partout dans le monde.

Analyse d'impact sur les activités stratégiques (SBIA)

L'analyse SBIA menée en 2018 a permis d'établir une liste d'activités que la haute direction a définies comme étant prioritaires pour assurer le rétablissement de l'activité en cas d'interruption, ainsi qu'une liste d'autres activités essentielles qu'elle a également qualifiées de prioritaires pour assurer le rétablissement de l'activité en cas d'interruption grave.

Une analyse d'impact sur les activités a été menée en 2018 et des processus et activités connexes de soutien ont été établies. Des plans de continuité des activités et de rétablissement TIC après une catastrophe ont été élaborés. L'analyse SBIA devrait être revue si l'organisation connaît des changements importants ou lorsque plusieurs années se sont écoulées.

L'analyse SBIA relève de la responsabilité du coordonnateur ORMS.

Évaluation des risques liés aux activités (BRA)

L'évaluation BRA pour l'organisation a été initialement menée en 2018 dans le cadre de l'analyse SBIA. L'évaluation BRA a été revue en décembre 2019. Elle devrait être revue chaque année ou si l'organisation connaît des changements importants, y compris en cas d'événement perturbateur grave. L'évaluation BRA relève de la responsabilité du coordonnateur ORMS.

Plan de continuité des activités (BCP)

Le plan BCP est le plan stratégique organisationnel pour l'UIT et toutes les unités qui la composent partout dans le monde. Il précise les rôles, les responsabilités et la structure pour ce qui est de la planification, de la prise de décision, de la coordination, de la communication et de l'échange d'informations pendant un événement perturbateur.

Le plan BCP est étayé par des plans de rétablissement de l'activité (ARP) qui contiennent les exigences opérationnelles et techniques détaillées grâce auxquelles les activités prioritaires et les autres activités essentielles visées par les plans ARP seront rétablies. Un plan devrait être prévu pour chaque unité opérationnelle.

Les plans ARP ont vocation à servir d'outils opérationnels, d'aide-mémoire contenant des informations essentielles relatives aux personnes, aux locaux et aux équipements à l'intention des responsables opérationnels après un événement perturbateur, ainsi que de solutions de continuité pour permettre une réponse et un rétablissement efficaces.

L'exécution des différents plans relèvera de la responsabilité des coordonnateurs BC des unités opérationnelles désignés par la direction. Tous les plans ARP seront revus chaque année. Le coordonnateur ORMS est chargé de la gestion des plans ARP.

# 2 Amélioration

Atténuation

Il y aura un programme planifié d'examen des pratiques de travail actuelles concernant les activités prioritaires afin de déterminer si des mesures pratiques efficaces sur le plan des coûts peuvent être identifiées pour prévenir et/ou atténuer les effets de l'événement perturbateur. La planification et le suivi du programme d'atténuation des effets grâce à l'évaluation BRA et à l'examen relèveront de la responsabilité du coordonnateur ORMS en coopération avec les coordonnateurs BC.

Ressources

Les besoins de ressources supplémentaires pour les mesures d'atténuation devraient être examinés chaque année et toutes les ressources doivent être clairement identifiées et justifiées.

Formation

La politique BC sera communiquée à l'ensemble du personnel, avec une formation appropriée et régulière sur la sensibilisation. Le système BCMS devrait être intégré dans les futures formations dispensées à l'entrée en fonction des fonctionnaires.

La formation relève de la responsabilité du coordonnateur ORMS.

Simulation

Une série de simulations théoriques BC sera organisée, idéalement tous les ans, par le coordonnateur ORMS en coopération avec le responsable TIC BC/DR.

# 3 Mise en œuvre

• Réponse et rétablissement.

• Activation et désactivation.

Le fonctionnaire auquel cette responsabilité a été déléguée sera chargé d'activer et de désactiver le plan BCP.

# 4 Examen

• Une vérification de la conformité, un suivi, une analyse et un audit seront effectués.

• Le coordonnateur ORMS est chargé de faciliter la vérification de la conformité, le suivi et l'audit, en liaison avec l'Unité de l'audit interne.

• Tout événement exigeant l'activation d'un plan ARP sera analysé afin d'en tirer des enseignements et des bonnes pratiques et de modifier les plans s'il y a lieu. De même, tout événement exigeant l'activation d'un plan de rétablissement TIC sera analysé afin d'en tirer des enseignements. Le coordonnateur ORMS sera chargé de veiller à ce que les analyses correspondantes soient menées, en coopération avec le responsable TIC BC/DR si le plan de rétablissement TIC après une catastrophe a été activé.

• Le système BCMS en général et le plan BCP en particulier doivent être revus chaque année.

• Le rétablissement TIC après une catastrophe est la capacité des éléments TIC d'une organisation à assurer leurs fonctions opérationnelles essentielles avec un niveau acceptable après une interruption dans un délai défini au préalable.

• Le rétablissement TIC après une catastrophe fait partie du système BCMS. Une politique de rétablissement TIC complète la politique BCP et, de la même manière, un plan global de rétablissement TIC après une catastrophe complète le plan BCP.

• Le plan de rétablissement TIC après une catastrophe est appuyé par les plans de rétablissement des services informatiques des unités opérationnelles (BITSRP) et par les plans de rétablissement des services informatiques du Département des services informatiques (ISDITRP), qui sont les plans techniques détaillés qui permettront le rétablissement après un événement perturbateur ayant des incidences directes sur les applications informatiques des unités opérationnelles ou sur l'infrastructure/l'environnement du Département des services informatiques, respectivement.

• Les plans BITSRP et ISDITRP sont revus chaque année.

• Le responsable TIC BC/DR est chargé de la gestion de ces plans techniques.

ANNEXE 2

Gestion des crises

La structure CM de l'organisation comprend les éléments suivants:

• Politique CM.

• Responsabilités pour la gouvernance.

• Désignation de l'Équipe de gestion des crises (CMT) et de l'Équipe de lutte opérationnelle (ORT).

• Lignes directrices et procédures opérationnelles normalisées (SOP).

• Programme de formation.

• Vérification de la conformité et examen a posteriori.

Des exercices de formation théoriques de l'Équipe CMT ont été menés en 2018 et 2019.

La structure CM est conçue pour les crises qui sont propres à l'UIT, sachant que le siège, les bureaux régionaux et les bureaux hors siège pourraient subir des crises impliquant d'autres institutions, fonds et programmes des Nations Unies nécessitant que d'autres organisations soient membres de l'Équipe CMT d'un lieu d'affectation.

Communication en cas de crise

La communication de l'organisation en cas de crise comprend deux éléments essentiels:

• La capacité des fonctionnaires, d'une part, de recevoir et d'envoyer des informations essentielles pour la sûreté et la sécurité 24 heures sur 24 et 7 jours sur 7 et, d'autre part, de demander d'urgence l'assistance de la Division SSD.

• L'existence au sein de l'organisation d'une structure efficace de communication institutionnelle interne et externe pendant la crise.

Communication en cas de crise pour les fonctionnaires

La Division SSD fournit une capacité opérationnelle de communication en cas de crise, au besoin en liaison avec le Département de la sûreté et de la sécurité de l'Office des Nations Unies à Genève ou avec les fonctionnaires du Département UNDSS basés sur les autres lieux d'affectation pertinents de l'UIT, ou dans les endroits où se tiennent des manifestations partout dans le monde.

Après avoir mené des essais pilotes et une évaluation, l'UIT a choisi d'établir un partenariat avec l'OIM et d'adopter l'utilisation du Réseau de communication et d'analyse de la sécurité (SCAAN) pour tous les fonctionnaires en poste dans les bureaux régionaux et les bureaux de zone, y compris au bureau de liaison à New York, les fonctionnaires du siège qui partent fréquemment en mission et tous les autres fonctionnaires du siège qui choisissent d'utiliser le système SCAAN.

L'application SCAAN offre, 24 heures sur 24 et 7 jours sur 7, une capacité et des fonctionnalités permettant de répondre aux besoins des fonctionnaires de l'UIT concernant les communications en cas de crise.

Communication institutionnelle en cas de crise

En ce qui concerne la communication institutionnelle interne et externe en cas de crise, le Chef de la Division de la communication stratégique (SCD) du Département de la planification stratégique et des relations avec les Membres (SPM) est un membre clé de l'Équipe CMT et joue un rôle important dans la fourniture sans délai d'orientations concernant la communication en cas de crise pour les membres de l'Équipe CMT, sur la base des bonnes pratiques appliquées actuellement en matière de communication en cas de crise par le système UNSMS et le Groupe de la communication des Nations Unies (UNCG) du Département de l’information des Nations Unies.

Des procédures opérationnelles normalisées pour la communication en cas de crise à l'intention des membres de l'Équipe CMT ont été rédigées et seront incorporées dans la politique et les lignes directrices CM.

Appui à la sécurité et intervention

La Division de la sûreté et de la sécurité de l'UIT (SSD), y compris les gardes en uniforme de l'entreprise prestataire Protectas, fournissent cette capacité au siège, au besoin en liaison avec la police de Genève et le Département de la sécurité et de la sûreté (DSS)/les services de sûreté et de sécurité (SSS) de l'ONU.

Pour les lieux d'affectation correspondant aux bureaux régionaux et aux bureaux de zone de l'UIT, et pour les manifestions mondiales ou régionales organisées par l'Union, le Chef de la Division SSD fournit la capacité de conseil et d'orientation concernant la sécurité, y compris l'évaluation des risques, et peut assurer la liaison avec les autorités du pays hôte s'occupant des situations d'urgence ou avec le personnel du système UNSMS au niveau local ou obtenir leur appui en matière de sécurité.

Mesures en cas d'incident avec de nombreuses victimes

Dans le cas d'une crise avec un grand nombre de victimes au siège, le premier triage paramédical effectué à l'UIT sera coordonné par le Chef de la Division SSD, avec le médecin-conseil et l'infirmière du Service médical ainsi que le conseiller du personnel, si tous sont en poste au moment où l'incident grave se produit.

En outre, il est probable que les services d'urgence du canton de Genève comprenant des urgentistes, des policiers et des pompiers se rendront sur les lieux et entreront dans les locaux de l'UIT après y avoir été autorisés par qui de droit. Le guide élaboré par l'ONUG pour la gestion des incidents faisant de nombreuses victimes a été utilisé par le médecin-conseil du Service médical, en liaison avec les autorités de santé du canton, pour rédiger les lignes directrices analogues propres à l'UIT.

Pour les lieux d'affection correspondant aux bureaux régionaux et aux bureaux de zone, ou pour les lieux où des manifestations UIT internationales ou régionales se tiennent, les accords de pays hôte et les plans de sécurité par zone des Nations Unies, ainsi que les plans de sûreté et de sécurité de la manifestation contiennent des dispositions analogues en la matière applicables aux fonctionnaires de l'UIT, aux délégués et aux visiteurs.

Gestion des crises − Appui aux fonctionnaires, aux survivants et à leurs familles

Pendant une crise, les fonctionnaires, les survivants et les familles, ainsi que les membres de l'Équipe CMT subiront inévitablement un stress bien supérieur que celui qu'ils subissent normalement et risquent donc d'avoir besoin de l'aide de spécialistes, à la fois pendant la crise et une fois celle-ci terminée.

Le conseiller du personnel est à la disposition des fonctionnaires, des survivants et de leurs familles au siège et dans les bureaux hors siège, pour leur fournir/coordonner le premier soutien nécessaire après une crise, ainsi qu'un soutien à moyen et long terme. Le conseiller du personnel a accès à un réseau qui est géré par le Groupe de gestion du stress traumatique relevant du Département de la sûreté et de la sécurité des Nations Unies.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_