CENTRE FOR CYBERSECURITY BELGIUM

LES MESURES DE CYBERSÉCURITÉ À METTRE EN OEUVRE

NIS 2 : approche « tous risques (*all hazards*) » qui vise à protéger les réseaux et les systèmes d'information ainsi que leur environnement physique contre les incidents. La loi impose de prendre des mesures appropriées et proportionnelles en fonction de l'analyse de risques de l'entité. Ces mesures portent au moins sur :

Les politiques relatives à l'analyse des risques et à la sécurité des systèmes d'information

La gestion des incidents

La continuité des activités et la gestion des crises

La sécurité de la chaîne d'approvisionnement

La sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information, y compris le traitement et la divulgation des vulnérabilités.

Une politique de divulgation coordonnée des vulnérabilités

Des politiques et des procédures pour évaluer l'efficacité des mesures de gestion des risques en matière de cybersécurité

Cyberhygiène et la formation à la cybersécurité

Des politiques et des procédures sur la cryptographie et, le cas échéant, du chiffrement

La sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs

Des solutions d'authentification à plusieurs facteurs, de communications sécurisées et de systèmes sécurisés de communication d'urgence au sein de l'entité, selon les besoins

Ces mesures de sécurité peuvent être implémentées avec les référentiels CyberFundamentals (CyFun®) ou ISO 27001.