Agence pour l'Evaluation de
la Qualité de l'Enseignement Supérieur

RAPPORT D'ÉVALUATION

Cluster Informatique

Master Cybersécurité

Université Libre de Bruxelles (ULB)
Université catholique de Louvain (UCLouvain)
Université de Namur (UNamur)
Haute École Bruxelles-Brabant (HE2B)
Haute École Libre de Bruxelles – Ilya Prigogine (HELB)
École Royale Militaire (ERM)

Pascal Marquet (président)
Thomas Tang
Noëmie Honoré
Alexandre Al Ajroudi

11 juillet 2023

Table des matières

Informatique : ULB-UCLouvain-UNamur-HE2B-HELB-ERM

Contexte de l'évaluation

L'Agence pour l'évaluation de la qualité de l'enseignement supérieur (AEQES) a procédé en 2022-2023 à l'évaluation du master en Cybersécurité. Dans ce cadre, les experts mandatés par l'AEQES se sont rendus les 1 et 2 décembre 2022 à l'Université Libre de Bruxelles (établissement référent pour l'organisation du master conjoint en Cybersécurité) sur le campus de La Plaine, accompagnés par Mathieu Lecouvet de la Cellule exécutive.

Le comité des experts a élaboré le présent rapport sur la base du dossier d'autoévaluation rédigé par les responsables du master et de la visite d'évaluation (observations, consultation de documents et entretiens). Au cours de cette visite, les experts ont rencontré des représentants des autorités académiques des établissements partenaires, des membres du personnel enseignant, des membres du personnel administratif, des étudiants du master, des diplômés et des représentants du monde professionnel.

Après avoir présenté aux établissements partenaires les principales conclusions de cette évaluation externe, le rapport revient plus en détail sur les constats, analyses et recommandations relatifs aux cinq critères du référentiel d'évaluation AEQES :

1 la gouvernance et la politique qualité
2 la pertinence du programme
3 la cohérence interne du programme
4 l'efficacité et l'équité du programme
5 la réflexivité et l'amélioration continue

Le rapport se clôture sur la conclusion de l'évaluation et se complète du droit de réponse formulé par les établissements impliqués dans l'organisation du master.

L'objectif de ce rapport est de fournir aux établissements des informations qui leur permettront d'améliorer la qualité du master en Cybersécurité. Il vise en outre à informer la société au sens large de la manière dont les établissements partenaires mettent en œuvre leurs missions.

Composition du comité[1]

- Pascal Marquet (président), expert en pédagogie et qualité au sein de l'enseignement supérieur
- Alexandre Al Ajroudi, expert étudiant
- Noëmie Honoré, experte de la profession
- Thomas Tang, expert pair

[1] Un bref résumé du *curriculum vitae* des experts est publié sur le site internet de l'AEQES : http://aeqes.be/experts_comites.cfm

Synthèse

FORCES PRINCIPALES

- Formation en co-diplomation, en adéquation avec la demande de compétences et les besoins du marché du travail
- Étendue des réseaux scientifiques et professionnels des enseignants
- Bonne visibilité et attractivité avérée de la formation
- Formation internationale, principalement dispensée en anglais
- Bonne insertion professionnelle des étudiants diplômés
- Bon encadrement des stages et des mémoires de fin d'études

FAIBLESSES PRINCIPALES

- Le comité de gestion ne s'est pas réuni depuis la crise sanitaire
- Dispersion des informations de scolarité sur les différents sites des établissements, multiplication des plateformes institutionnelles
- Déséquilibre homme-femme parmi les étudiants (7 % de femmes), et dans une moindre mesure parmi les enseignants
- Gestion administrative complexe et force de travail dédiée insuffisante
- Manque d'identification d'une personne responsable de la formation
- EEE réalisée par chaque établissement, sans coordination ni exploitation des informations à l'échelle du consortium
- Absence des partenaires socio-professionnels dans les instances de régulation de la formation
- Le plan d'action comporte des dates dépassées sans qu'il soit certain que les objectifs aient été atteints

OPPORTUNITÉS

- Formation unique sur le territoire de la FWB
- Caractère international de la formation qu'il est encore possible d'accroître
- Existence d'une passerelle vers le diplôme
- Croisement systématique des données produites par chaque établissement
- Se doter d'une vision prospective de la cybersécurité en s'appuyant sur les données de suivi de la formation et le milieu socio-professionnel

MENACES

- La coordination administrative et pédagogique entre les différents établissements est une source de difficultés
- L'évolution des enjeux de la cybersécurité pourrait être plus rapide que le rythme de révision du programme
- Certains étudiants ne terminent pas ou étalent leur formation après avoir été recrutés prématurément
- Le caractère multi-site est une source de désengagement potentiel des étudiants, en particulier ceux à mobilité réduite

RECOMMANDATIONS PRINCIPALES

1. Davantage impliquer les étudiants, le milieu socio-professionnel et les *alumni* dans les instances de régulation de la formation (comité de gestion, *Advisory Board*)
2. Introduire des éléments de démarche qualité dans la convention en cours de renouvellement
3. Formaliser une démarche d'évaluation et d'évolution du programme à l'échelle du consortium d'établissements
4. Rendre plus accessibles, voire centraliser les informations relatives à la vie de la formation (emploi du temps, syllabus, modalités d'évaluation, etc.)
5. S'assurer de la complétude des descriptifs des cours et des attendus du stage et du mémoire de fin d'études
6. Promouvoir la formation auprès d'un public plus féminin
7. Rendre la personne responsable de la formation et/ou les interlocuteurs plus identifiables
8. Davantage adapter la passerelle au parcours antérieur des étudiants
9. Réduire au maximum les contraintes de choix de cours consécutives à leur emprunt à d'autres formations
10. Mieux exploiter les informations en provenance de chaque établissement dans le pilotage de la formation
11. Introduire des modalités de suivi et de mise à jour du plan d'action plus serrées

Présentation des établissements et du programme évalué

L'Université libre de Bruxelles (ULB), établissement référent pour l'organisation du master en Cybersécurité, est une université complète créée en 1834. Elle couvre toutes les disciplines au travers de neuf facultés (Philosophie et Sciences sociales, Lettres, Traduction et Communication, Droit et Criminologie, *Solvay Brussels School of Economics and Management*, Sciences psychologiques et de l'Éducation, Architecture, Sciences, Médecine, École polytechnique de Bruxelles) et de trois entités d'enseignement et de recherche indépendantes des facultés (École de santé publique, Faculté des Sciences de la Motricité, Faculté de Pharmacie). Son organisation et sa recherche sont fondées sur le principe du libre examen. Elle est présente sur huit sites à Bruxelles et à Charleroi. L'ULB organise plus de 40 programmes de bachelier, 150 programmes de master et 65 masters de spécialisation. Le master en Cybersécurité qui fait l'objet de la précédente évaluation est rattaché à la faculté des sciences.

Créée en 1425, l'Université catholique de Louvain (UCLouvain) couvre l'ensemble des disciplines et accueille près de 35.000 étudiants. Elle cultive trois missions : l'enseignement, la recherche et le service à la société. Elle s'organise autour de sept sites, dont six campus ainsi que de 14 facultés. Elle propose 45 programmes de bacheliers et près de 200 masters (incluant les masters de spécialisation). L'UCLouvain dispense des formations à travers ses quatorze facultés : l'école polytechnique de Louvain ; la faculté d'architecture, d'ingénierie architecturale, d'urbanisme ; la faculté de droit et de criminologie ; la faculté de médecine et médecine dentaire ; la faculté de pharmacie et des sciences biomédicales ; la faculté de philosophie, arts et lettres ; la faculté de psychologie et des sciences de l'éducation ; la faculté de santé publique ; la faculté de théologie ; la faculté des sciences de la motricité ; la faculté des bioingénieurs ; la faculté des sciences ; la faculté des sciences économiques, sociales, politiques et de communication ; la *Louvain school of management.* Le master en Cybersécurité est rattaché à l'école polytechnique de Louvain.

Fondée en 1831, l'Université de Namur (anciennement Facultés Universitaires Notre-Dame de la Paix) est une association sans but lucratif reconnue par le décret du 7 novembre 2013 de la Fédération Wallonie-Bruxelles de Belgique. L'établissement a pour missions l'enseignement, la recherche et le service à la communauté. Elle accueille plus de 7000 étudiants et se structure autour de six facultés (Droit, Informatique, Médecine, Philosophie et lettres, Sciences, Sciences économiques, sociales et de gestion), une École des langues vivantes et un Département d'éducation et de technologie. L'Université est implantée au centre-ville de Namur. Le master en Cybersécurité est rattaché à la faculté d'informatique.

La Haute École Bruxelles-Brabant (HE2B) est issue en 2016 de la fusion de deux établissements : la Haute École de Bruxelles et la Haute École Paul-Henri Spaak. Elle est organisée et subventionnée par la Fédération Wallonie-Bruxelles (FWB). Son pouvoir organisateur est le réseau Wallonie-Bruxelles Enseignement. La Haute École se compose, autour d'une unité de direction centrale, de sept unités structurelles (Nivelles, Defré, ESI, ISIB, ISES, ISEK et IESSID) réparties sur dix implantations. Elle dispense 55 formations de type court et long dans dix domaines de formation différents sur les quatorze organisés par les hautes écoles en FWB. Les cours dispensés dans le cadre du master en Cybersécurité sont organisés au sein de l'École Supérieure d'Informatique (ESI).

La Haute École Libre de Bruxelles (HELB) - Ilya Prigogine appartient au réseau libre à caractère non confessionnel. Elle a été constituée en 1996 par la fusion de cinq institutions lors de la création des hautes écoles : l'École d'Infirmiers et Accoucheuses annexée à l'Université libre de Bruxelles, l'Institut Libre d'Enseignement Supérieur Économique et

Paramédical de Bruxelles, l'Institut Supérieur pour les Carrières Auxiliaires de la Médecine, l'Institut Supérieur des Sciences Humaines Appliquées - École Ouvrière Supérieure et l'Institut de Radioélectricité et de Cinématographie. La HELB – Prigogine regroupe plusieurs départements : social, santé, communication et médias audiovisuels et technologie et économie. C'est au sein de ce dernier département, situé sur le campus de la Plaine à Ixelles, que sont dispensés les enseignements du master en Cybersécurité.

L'École Royale Militaire, fondée en 1834, est une institution militaire d'enseignement supérieur assurant la formation des officiers de l'armée belge (composantes terre, air, marine et médicale). L'ERM organise des bacheliers et masters en sciences de l'ingénieur et en sciences sociales et militaires.

Le master en Cybersécurité est unique en Fédération Wallonie-Bruxelles. En 2019-2020, ce cursus comptait 87 étudiants, dont 7% de femmes.

Critère 1 : L'établissement/l'entité a formulé, met en œuvre et actualise une politique pour soutenir la qualité de ses programmes

CONSTATS ET ANALYSES

Dimension 1.1 : Politique de gouvernance de l'établissement

1. Le consortium, composé de six établissements (ULB-UCLouvain-UNamur-HE2B-HELB-ERM), a mis en place un ensemble de principes de gouvernance et de partage des responsabilités clair, consigné dans une convention datant de 2016, renouvelée en 2019, prorogée en 2022 et sur le point d'être renouvelée dans les prochains mois.

Dimension 1.2 : Gestion de la qualité aux niveaux de l'établissement, de l'entité et du programme

2. La démarche et les procédures qualité s'inscrivent dans les habitudes de fonctionnement de chacun des établissements, avec une double contrainte : être conforme à celle de l'établissement référent (politique qualité de l'ULB, procédure de révision des programmes, etc.) et pouvoir se décliner dans chaque établissement, notamment pour l'implémentation de l'évaluation des enseignements par les étudiants (EEE). Si cette approche est globalement fonctionnelle, elle requiert des efforts de coordination qui sont difficiles à fournir et qui suscitent actuellement une réflexion de la part des responsables de chaque établissement co-diplômant.

Dimension 1.3 : Élaboration, pilotage et révision périodique du programme

3. Un comité de gestion a été créé pour piloter le master, avec une composition équilibrée entre les établissements de la co-diplomation. Il constitue à la fois l'instance de pilotage et le jury qui se réunit chaque année et procède à la régulation du programme. Cette instance ne s'est pas réunie depuis la crise sanitaire et nécessite ainsi d'être relancée.
4. Le comité constate que si les étudiants peuvent, selon les établissements, être impliqués dans les instances qualité au niveau facultaire ou de l'entité-école, ils sont absents du comité de gestion du master cybersécurité. Dans la mesure où cette formation est majoritairement constituée de cours empruntés, les étudiants ne participent de fait pas aux réflexions et à l'amélioration du programme. Pour cette même raison, et du fait qu'ils ont pu se trouver en stage, les étudiants n'ont que très peu été impliqués dans l'exercice d'autoévaluation. Il n'y a, en outre, pas toujours de délégués étudiants représentant spécifiquement le master cybersécurité.
5. Il n'y a pas non plus d'autres parties prenantes, comme les partenaires socio-professionnels, participant aux instances de pilotage exclusivement dédiées au master cybersécurité (comité de gestion, etc.). L'éventuelle évolution du contenu du programme ne peut ainsi pas bénéficier d'un apport direct des employeurs potentiels des futurs diplômés.

6. Le comité observe que la co-diplomation est une source de difficultés en matière d'élaboration d'une démarche d'amélioration continue du programme, dont les enseignements dédiés sont peu nombreux (voir point 4 ci-dessus) et dont les autres enseignements ont leur vie propre au sein d'autres programmes, eux-mêmes soumis à des démarches de gestion de la qualité qui sont à la fois propres et particulières aux établissements qui les délivrent.

Dimension 1.4 : Information et communication interne

7. Chaque établissement possède ses propres canaux et flux d'information en direction des parties prenantes, et notamment des étudiants, ce qui nécessite un suivi et une coordination consommatrice de temps et source de retard dans la diffusion de l'information. A cet égard, le master cybersécurité est mentionné sur le site des différents établissements partenaires, en plus de posséder sa page dédiée.

RECOMMANDATIONS

1. Le renouvellement de la convention pourrait être l'occasion d'introduire des éléments relevant de la démarche qualité partagée par tous les établissements et à définir ensemble.
2. La composition du comité de gestion pourrait faire l'objet d'une révision avec l'introduction d'autres parties prenantes que les seuls académiques.
3. Une vision complète des démarches d'amélioration (EEE et autres démarches de recueil de données) de tous les enseignements intégrés au programme du master cybersécurité reste à construire, afin d'extraire les points de convergence et de divergence, qui constitueraient des leviers ou des obstacles à l'amélioration de la qualité du master cybersécurité.
4. Le comité recommande de davantage centraliser l'information et d'utiliser la page dédiée https://masterincybersecurity.ulb.ac.be/ comme point d'entrée principal du programme, y compris après la phase de promotion de la formation et d'inscription. Une éventuelle autre plateforme commune pourrait être envisagée comme lieu dédié à la diffusion et à la mise à jour des informations relatives au programme et à son organisation pratique.

Critère 2 : L'établissement/l'entité a développé et met en œuvre une politique pour assurer la pertinence de son programme

CONSTATS ET ANALYSES

Dimension 2.1 : Appréciation de la pertinence du programme

1. Le Master cybersécurité répond à des enjeux sociétaux forts. Le nombre d'inscrits est en hausse constante depuis sa création. Le taux d'employabilité des étudiants est très élevé. Le programme est construit dans le respect des dispositions légales. Fruit d'une collaboration entre six institutions belges, il délivre un programme qui traite de l'ensemble des thématiques de cybersécurité (aspects techniques, organisationnels, humains et juridiques) pour former des étudiants et leur permettre une bonne insertion dans le monde professionnel. Le programme est construit sur la base d'une majorité de cours de spécialité empruntés à chacune des institutions. Quelques cours ont été créés spécifiquement pour ce master.
2. L'évaluation du master par les étudiants est réalisée pour chaque enseignement, et ce par l'institution qui en a la charge. Aucune vue consolidée de l'ensemble des évaluations n'est disponible à ce jour, ce qui ne facilite pas l'analyse de la pertinence du programme et la proposition d'éventuels changements à l'échelle de la formation. Tout changement structurant du programme est validé par le comité de gestion. Le programme n'a cependant pas fait l'objet de révision depuis le dernier comité de gestion qui, comme cela a déjà été mentionné, a été organisé avant la crise du Covid-19.
3. Cela dit, des changements mineurs peuvent intervenir à l'échelle des enseignements à l'initiative des enseignants, très engagés et passionnés par leur sujet. Ces changements reposent le plus souvent sur l'expertise et le réseau de contacts de chaque enseignant qui ajuste son cours au fil du temps. Les académiques disposent en effet d'un réseau de contacts en cybersécurité et font bénéficier leurs étudiants de l'expertise de ces personnes ressources au sein de leur(s) cours, par des interventions spécifiques ainsi que pour des mises en relation dans le processus de recherche d'un stage.

Dimension 2.2 : Information et communication externe

4. Un site web dédié est disponible pour fournir aux étudiants potentiels une série d'informations utiles (programme, modalités d'inscription, contacts, etc.).
5. La participation à des événements de promotion des masters et l'organisation de journées portes ouvertes permet de communiquer sur l'existence du master cybersécurité auprès des étudiants. Les enseignants se chargent également de fournir les éléments d'information nécessaires à la mise en œuvre par les institutions d'actions de promotion des programmes d'études.
6. Le nombre d'inscrits au master est actuellement satisfaisant du point de vue des responsables académiques en charge du pilotage du programme. En tant que seule formation de ce type en Fédération Wallonie-Bruxelles, le comité regrette néanmoins

qu'il n'y ait pas d'ambition en matière d'attractivité d'un plus grand nombre d'étudiants.

7. La part des femmes parmi les inscrits au master cybersécurité est très faible et se situe autour de 7%. Aucune action particulière n'est actuellement envisagée pour inciter des étudiantes à rejoindre ce master.

RECOMMANDATIONS

1. La cybersécurité étant un domaine en constante évolution, le comité d'experts recommande une révision annuelle du programme avec la participation de l'ensemble des parties prenantes (équipe pédagogique, représentants du milieu professionnel, *alumni*), pour vérifier l'adéquation des enseignements et compétences aux besoins du marché et des enjeux sociétaux.
2. La mise en place d'une évaluation du programme dans son ensemble (en complément des évaluations par enseignement par chacune des institutions) serait intéressante afin de disposer d'une vision centralisée de l'évaluation par les étudiants, et accessible aux équipes pédagogiques des six institutions. Cette évaluation permettrait de proposer des ajustements qui pourraient être discutés en comité de gestion.
3. Le Comité encourage les représentants du master, ses étudiants et ses *alumni* à participer à des actions de promotion du secteur de la cybersécurité auprès des étudiants et notamment du public de l'enseignement secondaire, pour promouvoir la diversité dans ce secteur, y compris de genre, et attirer davantage d'étudiants.

Critère 3 : L'établissement/l'entité a développé et met en œuvre une politique pour assurer la cohérence interne de son programme

CONSTATS ET ANALYSES

Dimension 3.1 : Acquis d'apprentissage du programme

1. Les institutions indiquent dans le dossier d'autoévaluation (DAE) avoir formulé et publié les acquis d'apprentissages du programme d'études. Les fiches présentes dans le catalogue et accessibles à l'adresse https://www.ulb.be/fr/programme/ma-secu-1#programme ne sont toutefois pas toutes renseignées ou mises à jour.
2. Le comité a pu relever certaines difficultés pour les étudiants à prendre connaissance du contenu des modules dont les fiches ne sont pas toujours renseignées. Le contenu et les acquis d'apprentissage semblent cependant, pour un certain nombre d'enseignements, spécifiés par les enseignants lors du premier cours.

Dimension 3.2 : Contenus, dispositifs et activités d'apprentissage qui permettent d'atteindre les acquis visés

3. La majorité des enseignements sont délivrés en anglais, qui est la langue de travail dominante dans le domaine de la cybersécurité. Les institutions mettent en œuvre des dispositifs d'aide linguistique et adaptent les modalités d'examens pour les étudiants non francophones, notamment pour les cours de la passerelle qui restent en langue française.
4. Un stage obligatoire de minimum 10 semaines doit être réalisé par les étudiants au cours du master. Il permet de compléter le volet académique de la formation par une expérience au sein du milieu professionnel. La présence de ce stage est un atout fort pour garantir la bonne insertion professionnelle de l'étudiant.
5. Le programme laisse une grande autonomie aux étudiants pour la recherche de leur stage et la définition de leur sujet de mémoire. Une liste des lieux de stage possibles existe, mais celle-ci ne semble pas être connue des étudiants.
6. Les attendus du mémoire de fin d'études ne semblent pas suffisamment définis en début de formation, ce qui peut être à l'origine d'une certaine forme de stress au fur et à mesure que l'échéance se rapproche. Le mémoire reste l'élément du programme que les étudiants diffèrent lorsqu'ils étalent leur formation sur plus d'années que ne le prévoit le programme.

Dimension 3.3 : Agencement global du programme et temps prévu pour l'atteinte des acquis d'apprentissage visés

7. Les enseignants ont construit un programme bien agencé et cohérent sur la base d'une grande majorité de cours d'emprunt, dispensés dans le cadre d'autres formations des six établissements associés. Toutefois, les difficultés de coordination et d'organisation multi-partenariales complexifient toute évolution de cet agencement.

8. Le programme tient compte des contraintes de déplacement des étudiants entre des campus distincts en regroupant les modules dispensés sur un site sur une même journée. Cependant, les modifications éventuelles des horaires des modules ne sont pas toujours mises à jour et concertées, engendrant certaines complications, comme par exemple le chevauchement horaire de deux cours.

Dimension 3.4 : Évaluation du niveau d'atteinte des acquis d'apprentissage visés

9. Les critères et modalités d'évaluation sont établis en cohérence avec les enseignements. Ceux-ci semblent par ailleurs communiqués de façon explicite par les enseignants pendant les cours. De même, les informations pratiques relatives à l'organisation des examens sont accessibles via le portail de l'ULB.

RECOMMANDATIONS

1. Le comité recommande de s'assurer de la complétude et de la mise à jour des informations liées aux contenus des enseignements et aux acquis d'apprentissage correspondants, qui sont mises à disposition des étudiants sur le catalogue et qui leur sont nécessaires pour construire leur Programme Annuel de l'Etudiant. Le catalogue devrait aussi préciser pour chaque enseignement les informations relatives aux critères et aux modalités d'évaluation.
2. Il est recommandé de mettre à disposition des étudiants ou de rendre plus accessible une liste des lieux de stage potentiels.
3. Les attendus du mémoire de fin d'études ainsi que ses modalités générales d'accompagnement, qui peuvent varier d'un enseignant à un autre, mériteraient d'être davantage formalisés, communiqués et explicités aux étudiants.
4. La nécessité de conduire des enseignements sur plusieurs sites impose de mettre à disposition des étudiants des informations mieux actualisées afin qu'ils puissent à la fois planifier leur programme de travail en fonction des éventuelles modifications apportées par chaque établissement ou d'imprévus.

Critère 4 : L'établissement/l'entité a développé et met en œuvre une politique pour assurer l'efficacité et l'équité de son programme

CONSTATS ET ANALYSES

Dimension 4.1 : Ressources humaines (affectation, recrutement, formation continuée)

1. Les enseignements sont assurés par une équipe de qualité et engagée : enseignants-chercheurs reconnus dans leur domaine de spécialité, experts issus du monde professionnel, intervenants exerçant également dans le monde professionnel.
2. Une seule personne est chargée de la gestion administrative de la scolarité au sein de l'établissement référent sans que son temps équivaille à un temps plein. La multiplication des tâches administratives, provoquée par la configuration multi-site, génère cependant des temps de réalisation des tâches ou de traitement des requêtes plus longs que pour une formation localisée sur un seul site.
3. Il n'y a pas de responsable pédagogique clairement identifié par les étudiants pour les aider en cas de difficultés. Le président du jury joue ce rôle mais les étudiants ne semblent pas être au courant.

Dimension 4.2 : Ressources matérielles (matériaux pédagogiques, locaux, bibliothèques, plateformes TIC)

4. Le nombre élevé de plateformes spécifiques à chaque établissement apparaît comme une source de confusion pour toutes les parties prenantes de cette formation.
5. Les ressources matérielles (locaux, équipements informatiques, etc.) sont adaptées à la formation. Les étudiants bénéficient en outre d'un accès aux différentes bibliothèques.
6. Le caractère multisite de la formation est une source potentielle d'absentéisme des étudiants, ainsi qu'un réel frein pour des étudiants en situation de mobilité réduite.

Dimension 4.3 : Équité en termes d'accueil, de suivi et de soutien des étudiants

7. Un grand nombre de cours sont dispensés en anglais, ce qui confère un caractère international à la formation, tandis que d'autres le sont en français, en particulier ceux qui composent les passerelles d'accès au master. Cependant, cela peut constituer un frein pour un public ne maîtrisant pas l'anglais ou pour un public non-francophone amené à suivre certains enseignements de passerelle en français.
8. Au cours de leur stage, les étudiants sont soutenus de façon régulière par un enseignant de la formation à travers un point de suivi par mail.
9. Les étudiants sont accompagnés par un enseignant-promoteur tout au long de leur travail de mémoire de fin d'études.

10. Concernant l'accès aux différentes plateformes en ligne propres à chacun des établissements partenaires, le caractère à la fois multi-établissement et multi-site de la formation crée de la complexité et une charge de travail supplémentaire pour les étudiants, qui doivent comprendre et s'adapter au fonctionnement et à la culture de travail propres à chaque établissement, sans toujours bénéficier suffisamment rapidement à la suite de l'inscription administrative au sein du cursus des accès, informations et ressources nécessaires spécifiques à chaque établissement.
11. L'existence d'une passerelle permet à des étudiants de se mettre à niveau avant de commencer la formation. Cette passerelle ne semble toutefois pas suffisamment souple, c'est-à-dire ajustée dans le contenu des cours qui la composent au parcours antérieur de l'étudiant.

Dimension 4.4 : Analyse des données nécessaires au pilotage du programme

12. L'établissement référent produit et exploite des données générales sur le nombre d'étudiants inscrits, les statistiques de réussite, la durée moyenne de la formation, etc. Une enquête sur l'insertion professionnelle des diplômés complète ces données. D'autres données sont collectées par les autres établissements, mais il n'y a pas de croisement systématique de ces informations, ni d'exploitation globale à des fins de pilotage.
13. C'est le cas aussi pour l'EEE qui est pratiquée par tous les établissements, sans que les informations recueillies ne soient transmises à l'ensemble des établissements ou ne soient centralisées.
14. Le jury annuel reste le seul moment institutionnel au cours duquel les enseignants discutent du programme. Il est en principe doublé d'une réunion du comité de gestion, lequel n'a cependant, comme dit précédemment, pas fonctionné depuis la crise sanitaire.

RECOMMANDATIONS

1. Compte tenu de la complexité et de la charge administrative que requiert la gestion de la scolarité et de l'emploi du temps de la formation, le comité recommande de dédier davantage de quotité de temps de travail à cette seule formation.
2. Il est important que les étudiants puissent avoir un interlocuteur académique identifiable, à l'échelle de chaque établissement ou à l'échelle de la formation, en particulier pour les étudiants étrangers qui ne sont pas familiers des modalités propres à l'enseignement supérieur en Fédération Wallonie-Bruxelles.
3. Le comité préconise d'optimiser, voire d'harmoniser les différents outils numériques mis à la disposition des étudiants afin de simplifier et d'accélérer l'accès à l'information.
4. Il apparaît nécessaire de fournir aux étudiants un agenda unique avec une mise à jour en temps réel des modifications des horaires des cours.
5. Il conviendrait aussi de rendre possible toutes les combinaisons de choix de cours en réduisant au maximum l'incompatibilité horaire entre certains cours en raison de leur superposition dans des établissements différents.

6. Le consortium gagnerait en unité si les étudiants pouvaient disposer d'un document unique d'information sur le fonctionnement de chaque établissement ainsi que d'un portail ou d'un LMS (*Learning Management System*) unique.
7. Le comité recommande que la passerelle puisse être davantage individualisée en fonction du parcours antérieur de l'étudiant.
8. Les différentes données récoltées par les établissements mériteraient d'être mises en correspondance et en cohérence à des fins de pilotage.

Critère 5 : L'établissement/l'entité a établi l'analyse de son programme et construit un plan d'action visant son amélioration continue

CONSTATS ET ANALYSES

Dimension 5.1 : Méthodologie de l'autoévaluation

1. Le DAE est le fruit d'une élaboration centralisée, mais fondée sur une démarche participative, à laquelle ont participé tous les établissements partenaires, les enseignants et, dans une moindre mesure, les étudiants. N'ont pas été consultés les employeurs potentiels et plus largement les partenaires socio-professionnels qui offrent des lieux de stage aux étudiants.
2. La collecte d'informations s'est révélée complexifiée par la multiplication des sources et des procédures propres à chaque établissement et leur croisement systématique n'a pas pu être réalisé.

Dimension 5.2 : Analyse SWOT

3. La SWOT consignée dans le DAE est la fusion de plusieurs SWOT réalisées en amont. Elle est lucide et pointe des aspects qui ont été confirmés par la visite. Certains points forts ou faibles ont aussi pu être mis en avant, comme parmi les points forts la position dominante du master dans l'offre de la Fédération Wallonie-Bruxelles (FWB) et la co-diplomation ; et parmi les points faibles, la faible représentation des parties prenantes internes dans les instances.

Dimension 5.3 : Plan d'action et suivi

4. Un plan d'action structuré en quatre axes a été élaboré (1 : coordination et pilotage du programme ; 2 : cohésion enseignants/étudiants ; 3 : actions pédagogiques ; 4 : visibilité et attractivité du programme). Les axes sont déclinés en objectifs clairs, en actions concrètes, avec des responsabilités identifiées, certes de manière générale, mais assorties de livrables avec des indications d'échéances. Certaines échéances sont cependant déjà dépassées, et ce sans qu'il soit certain que les objectifs ou les actions correspondants aient été menés à bien.

RECOMMANDATIONS

1. Compte tenu du caractère porteur de la formation d'un point de vue professionnel, de la dimension stratégique propre au domaine de la cybersécurité, ainsi que de l'évolution rapide de la discipline et des technologies associées, le comité recommande de réfléchir à comment introduire, à l'un ou l'autre moment dans le processus de pilotage du programme le point de vue des milieux professionnels. L'éventuelle opportunité d'une instance surplombante, comme un *Advisory Board/*Conseil d'orientation, pourrait être discutée.

2. La nature et la spécificité des informations nécessaires au pilotage mériterait une discussion collective, pour déterminer jusqu'à quel point ce que peuvent fournir les cours empruntés à des programmes préexistants est suffisant et à partir de quand des éléments spécifiques sont nécessaires. Il conviendrait aussi d'améliorer l'échange d'informations entre les établissements.
3. Le comité recommande de reprendre le plan d'action à la lumière des échanges de la visite avec des échéances tenables et des responsabilités mieux définies.

Conclusion

Le master en Cybersécurité répond à un besoin de la société belge en matière de formation de professionnels de haut niveau, que le consortium constitué de six établissements se propose de couvrir. C'est à la fois un atout en matière de mise en commun de compétences et de positionnement dans l'offre de formation de la FWB. Cela n'est néanmoins pas sans poser un certain nombre de défis en matière d'organisation, de coordination et de cohérence des parcours de formation. Au terme des premières années d'existence, le master s'est imposé comme un programme à sceaux multiples visible et reconnu, à l'issue duquel les étudiants trouvent à s'insérer professionnellement sans difficulté.

L'exercice d'autoévaluation et la visite ont montré que la mise en place du programme était désormais réalisée et que chacune des parties prenantes s'en était construit une représentation spécifique : l'équipe de gouvernance a une vision claire des enjeux de positionnement et des difficultés de coordination ; les enseignants sont animés par le désir de contribuer à un programme inédit et pertinent ; les étudiants bénéficient des avantages de la co-diplomation. Il manque à ces parties prenantes les professionnels qui sont à ce jour les grands absents sur le plan formel, indépendamment du fait que les enseignants apportent à ce programme la force de leur propre réseau.

La phase qui s'ouvre se présente comme une nouvelle étape de consolidation du programme, avec des enjeux de formalisation qui restent à relever : à court terme, mise en commun du pilotage et de la démarche qualité, et montée en gamme du travail de coordination dans la gestion et l'organisation du cursus ; à moyen terme, renforcement de la vision stratégique, notamment eu égard au positionnement de la formation aux niveaux national et international.

Droit de réponse de l'établissement

ULB

Évaluation complète
Informatique – Master conjoint en Cybersécurité

2022-2023

Droit de réponse de l'établissement évalué

Commentaire général éventuel :

☒ L'établissement ne souhaite pas formuler d'observations de fond

Partie du rapport (1,2,3,4,5) n° de page, n° §	Observation de fond

UNIVERSITÉ DE NAMUR — UCL Université catholique de Louvain — ULB UNIVERSITÉ LIBRE DE BRUXELLES — HELB Ilya Prigogine — HE2B HAUTE ÉCOLE BRUXELLES-BRABANT

Nom, fonction et signature de l'autorité académique dont dépend l'entité

Olivier Markowitch, Doyen de la Faculté des Sciences

Nom et signature du coordonnateur de l'autoévaluation

Héléna Bruyninckx, Coordonnatrice de l'évaluation

Helena Bruyninckx (Authentication)

Digitally signed by Helena Bruyninckx (Authentication)
Date: 2023.06.16 09:25:45 +02'00'