International Federation of Biosafety Associations

www.InternationalBiosafety.org

Certification Professionnelle en Cyber biosûreté

Contenu de l'Examen, Exemples de questions & Références

La Certification Professionnelle (CP) en Cyber biosûreté de l'IFBA identifie les individus ayant démontré des compétences dans la mitigation des risques de cybersécurité au sein des laboratoires biologiques. Cela inclut les risques liés aux Technologies de l'Information (TI) et aux Technologies Opérationnelles (TO), dans le but de protéger les recherches biologiques sensibles, les données, les bases de données, ainsi que les installations et équipements de laboratoire contre tout accès illicite ou non autorisé, vol, altération ou autres formes de mauvaise utilisation.

La CP en Cyber biosûreté convient à un large éventail de professionnels travaillant dans et autour des laboratoires biologiques, de la biotechnologie, des laboratoires pharmaceutiques et de recherche, tels que les conseillers en gestion des risques biologiques, les responsables de la biosécurité, le personnel scientifique de laboratoire, les technologistes biomédicaux, les professionnels des technologies de l'information et de la cybersécurité, le personnel d'exploitation et de maintenance des installations, le personnel de sécurité, la direction et l'administration.

Aux fins de cette certification, la Cyber biosûreté est définie comme "la protection et la mitigation de l'abus, de l'exploitation, des dommages ou des perturbations des informations précieuses, des données, des bases de données, des équipements et des installations à l'interface du laboratoire biologique, des installations connexes en sciences de la vie et des mondes numériques."

Le Corps de Connaissances (Body of Knowledge « BOK ») ci-dessous identifie 5 domaines (thématiques) et 45 connaissances / déclarations de tâches qui définissent la compétence requise pour la certification en Cyber biosûreté. Le contenu de l'examen est basé sur ce BOK et chaque question de l'examen est liée à l'une des déclarations ci-dessous.

Domaine A – Concepts de Cyber biosûreté

1. Décrire le domaine émergent de la cyber biosûreté, à l'interface entre la cyber sécurité, la cyber sécurité physique, la gestion de la qualité, la biosécurité et la sûreté biologique.
2. Décrire les menaces et les vulnérabilités associées à la cyber biosûreté dans de nombreux secteurs distincts des sciences de la vie, des sciences biomédicales, de la biotechnologie, de la biologie synthétique et d'autres aspects de la bioéconomie.

3. Identifier les façons dont les vulnérabilités liées à la cyber biosûreté dans les laboratoires biologiques présentent un risque pour l'intégrité des matériaux biologiques et des données numériques associées, les travailleurs de laboratoire, la communauté publique environnante, les animaux, et l'environnement.
4. Comprendre comment les dispositifs et équipements de mise en réseau exacerbent les vulnérabilités et les risques de cyber biosûreté, et comment réduire ces risques (par exemple, séparer les dispositifs moins sécurisés du réseau, retirer les dispositifs de l'Internet des Objets « internet of things: IoT » qui ne sont pas critiques ou sécurisés).
5. Savoir comment identifier, évaluer, réduire et répondre aux menaces, aux risques et aux incidents de cyber biosûreté dans les laboratoires biologiques, associés à leurs actifs avec des composants numériques, des équipements en réseau, des appareils et les systèmes dans les installations.
6. Comprendre les rôles et responsabilités du personnel clé dans la cyber biosûreté (par exemple, les responsables de la biosécurité, les scientifiques de laboratoire, le personnel d'entretien des installations, le personnel informatique, l'administration, la sécurité), ainsi que l'importance d'une communication régulière entre ces derniers.
7. Savoir comment élaborer et mettre en œuvre des programmes de formation en cyber biosûreté, promouvoir la sensibilisation à la cyber biosûreté, et encourager les bonnes pratiques de cybersécurité personnelle dans l'environnement de travail du laboratoire.
8. Être familiarisé avec et comprendre comment élaborer/mettre à jour des politiques organisationnelles et des procédures opérationnelles standard en accord avec les meilleures pratiques pertinentes de cyber biosûreté.

Domaine B – Les Fondamentaux de la Cybersécurité

9. Essayer de comprendre quelles seraient les options disponibles pour un adversaire pour qu'il puisse mener une surveillance physique et cybernétique d'une installation dans le cadre d'objectifs qui pourraient être subtils, indirects ou inattendus, et comment réduire ces risques potentiels.
10. Comprendre les tactiques et techniques d'intrusion pouvant être utilisées par un adversaire pour accéder à/et exploiter des données et des systèmes (par exemple, l'ingénierie sociale, les **failles d'exploitation zero-day**, les compromissions de la chaîne d'approvisionnement logicielle, les réseaux, le stockage en nuage, les utilisateurs, les e-mails, les applications Web, les portails d'accès à distance, les appareils mobiles).
11. Définir les termes : Technologie de l'Information (TI), Technologie Opérationnelle (OT) et Internet des Objets (IoT).
12. Décrire les 3 catégories courantes d'authentification multifactorielle (c'est-à-dire connaissance, possession, inhérence).
13. Comprendre les principes du contrôle d'accès (par exemple : protection de la vie privée et des données dès la conception, une politique d'utilisation acceptable,

comptes utilisateur les moins privilégiés, configuration des comptes utilisateur et des autorisations de sécurité dans plusieurs environnements, gestion des droits numériques).

14. Comprendre les principes de gestion des identités et des accès (par exemple, gestion des permissions des entités et des groupes, configuration des unités organisationnelles et des objets).
15. Comprendre les principes de protection physique (par exemple, établissement de contrôle d'accès physique) et de protection des médias (par exemple, désinfection ou destruction appropriée des médias).
16. Comprendre les principes de protection des systèmes et des communications (par exemple, surveillance des dispositifs de limites externe et interne, mise en œuvre de sous-réseaux).
17. Comprendre les principes de l'intégrité des systèmes et des informations (par exemple, identification des problèmes système, déploiement de signatures réseau/hôte, réalisation de scans antivirus périodiques).

Domaine C – Risques liés aux Technologies de l'Information (TI) dans les Laboratoires Biologiques

18. Décrire les différents types de données stockées et transmises via les plates-formes et équipements de technologie de l'information dans le laboratoire biologique, et qui pourraient constituer un flux de données intéressant pour les adversaires.
19. Comprendre comment les vulnérabilités des données affectent négativement la gestion de la qualité en raison de la perte de confidentialité (c'est-à-dire la perte de données), la perte de disponibilité (c'est-à-dire la perturbation opérationnelle) et la perte d'intégrité (c'est-à-dire les données altérées).
20. Décrire comment l'exfiltration des données peut se produire à la fois par un adversaire interne et externe et comment les technologies de chiffrement de base de données peuvent être utilisées pour sécuriser les informations dans les bases de données biologiques.
21. Décrire les façons dont l'équipement de laboratoire en réseau pourrait être exploité à distance/digitalement pour compromettre l'intégrité de la recherche, altérer les séquences génomiques, manipuler les caractéristiques des agents biologiques et créer des produits biologiques nocifs.
22. Décrire comment l'utilisation de zones démilitarisées et de zones de confiance peut être utilisée pour renforcer la sécurité des équipements de laboratoire en réseau et des l'infrastructures.
23. Décrire comment les algorithmes de cryptographie pourraient être exploités pour l'utilisation de mots de passe, l'authentification multi-facteurs, le réseau privé virtuel et le chiffrement des données au repos et en transit, et comment ils peuvent être incorporés dans la politique de cyber biosûreté d'un laboratoire.

24. Comprendre l'importance de l'exploitation des évaluations périodiques des vulnérabilités et des tests de pénétration de réseau/application ciblés, pour identifier et atténuer les vulnérabilités.
25. Savoir comment réduire les vulnérabilités de cyber biosûreté présentées par l'utilisation de dispositifs personnels (par exemple, ordinateurs portables personnels et téléphones portables) pour accéder aux systèmes liés au laboratoire.
26. Comprendre les vulnérabilités associées à l'utilisation des technologies du spectre sans fil et des équipements connectés à Internet, et comment les dispositifs sans fil peuvent augmenter votre surface d'attaque et permettre de nouveaux vecteurs d'attaque pour les adversaires.
27. Décrire quelles vulnérabilités et quelles informations sensibles peuvent être révélées aux adversaires à travers des documents de contrôle administratif (par exemple : procédures d'intervention d'urgence, plans de programme de sécurité), des documents de budget et de planification, des documents de contrat, des plans d'étage et des schémas de laboratoires, des salles de soutien et des espaces mécaniques.
28. Décrire les moyens de restreindre la divulgation d'informations sensibles et de vulnérabilités des installations aux entrepreneurs de maintenance extérieurs, aux fournisseurs de services d'équipements et aux vendeurs.
29. Comprendre les vulnérabilités de cybersécurité associées aux systèmes de mise en réseau de la gestion des inventaires des agents pathogènes, et aux systèmes de gestion de l'information au laboratoire.
30. Savoir comment identifier et atténuer les vulnérabilités des activités menées par le personnel au laboratoire, et pouvant entraîner la divulgation d'informations sensibles (par exemple, partage légitime de données pour la recherche, l'enseignement ou des fins commerciales).

Domaine D – Risques liés à la Technologie Opérationnelle (OT) dans les Laboratoires Biologiques

31. Comprendre comment l'innovation technologique dans les "laboratoires intelligents" (c'est-à-dire les laboratoires dotés de dispositifs en réseau capables de surveillance et de contrôle à distance, de clés intelligentes) est sujette à des vulnérabilités de cybersécurité.
32. Comprendre les vulnérabilités de cybersécurité liées à l'utilisation de cahiers de laboratoire électroniques et d'assistants personnels virtuels pilotés par la voix utilisant des commandes vocales dans le laboratoire.
33. Savoir comment les systèmes de gestion automatisée des bâtiments en réseau et les logiciels de gestion de l'énergie sont sujets à des vulnérabilités de cybersécurité.
34. Décrire les façons dont un système de contrôle d'accès physique d'un laboratoire pourrait être exploité à distance/digitalement pour compromettre la sécurité.
35. Décrire les façons dont un système de gestion automatisée du bâtiment d'un laboratoire de confinement biologique pourrait être exploité à distance/digitalement

pour compromettre la biosécurité, le confinement, la sécurité de la vie et l'intégrité des données liées aux matériaux biologiques.

36. Décrire les façons dont les systèmes et équipements de décontamination d'un laboratoire biologique pourraient être exploités à distance/digitalement pour compromettre la biosécurité et le confinement biologique.
37. Décrire les façons dont les salles d'hébergement pour animaux de laboratoire et les systèmes de confinement des cages pourraient être exploités à distance/digitalement, ainsi que les impacts potentiels d'une telle intrusion.
38. Comprendre les risques potentiels de cybersécurité qui pourraient compromettre la chaîne d'approvisionnement d'un laboratoire et comment ces risques peuvent être réduits au minimum et inversés s'ils sont détectés.

Domaine E – Préparation et Réponse aux Incidents de Cyber biosûreté

39. Savoir comment effectuer une visite complète de l'installation dans le but d'élaborer un plan de mitigation des menaces de cyber biosûreté et de réponse aux incidents.
40. Décrire l'élaboration d'un plan complet de mitigation des menaces de cyber biosûreté, de réponse aux incidents et de communication pour minimiser les dommages, contenir la menace et maintenir la biosécurité et la biosûreté.
41. Comprendre les rôles et responsabilités du personnel clé en vue de répondre aux incidents de cyber biosûreté à la fois au sein de l'institution, ainsi que ceux provenant de spécialistes externes.
42. Savoir à l'avance où obtenir une assistance supplémentaire de confiance et vérifiée pour identifier, répondre et se remettre des incidents de cyber biosûreté.
43. Savoir quand et comment impliquer les entités chargées d'application de la loi pour répondre, enquêter, recueillir des preuves probantes et mener des entretiens.
44. Connaître les canaux de communication, comment signaler, et à qui, les incidents de cyber biosûreté potentiels détectés.
45. Savoir comment mener des exercices réguliers de l'équipe de réponse aux incidents de cyber biosûreté, y compris des exercices pratiques au laboratoire.

Plan de l'examen

Dans ce qui suit, vous avez une représentation du nombre de questions incluses dans chaque domaine de l'examen :

Plan d'Examen Certification Professionnelle en Cyber biosûreté Score de réussite – 70%	
Domaine	**Nombre de Questions**
A) Concepts de Cyber biosûreté	19
B) Les Fondamentaux de la Cybersécurité	18
C) Risques liés aux Technologies de l'Information (TI) dans les Laboratoires Biologiques	28
D) Risques liés à la Technologie Opérationnelle (OT) dans les Laboratoires Biologiques	12
E) Préparation et Réponse aux Incidents de Cyber biosûreté	13

Exemple de questions

Afin de familiariser les candidats avec la nature et la forme des questions d'examen, les exemples suivants sont fournis. Un astérisque marque la réponse correcte.

1. Quel scénario REPRÉSENTE LE MIEUX une préoccupation liée à la cyber biosûreté dans l'environnement actuel des laboratoires biologiques?
    A. Des laboratoires mal sécurisés pourraient permettre à des individus non autorisés de gagner accès et de voler des agents pathogènes des congélateurs du laboratoire.
    B. Des équipements de laboratoire et des appareils trop connectés à Internet pourraient être piratés pour accéder et modifier des données confidentielles du laboratoire. *
    C. Des chercheurs en laboratoire pourraient vendre des informations et des données scientifiques exclusives à une organisation de recherche concurrente.
    D. Les déchets pourraient être inadéquatement décontaminés avant de quitter le laboratoire pour être éliminés hors site.

2. Complétez cette déclaration: Utiliser _____ pour vérifier l'identité d'un utilisateur du réseau est un exemple d'authentification à facteurs multiples pour diminuer la probabilité d'une cyberattaque.
    A. un mot de passe et un nom d'utilisateur
    B. une question de sécurité et un code PIN
    C. un code à 4 chiffres à usage unique envoyé via SMS*
    D. un scan d'empreinte digitale et une reconnaissance faciale

3. Le département informatique élabore une politique et des procédures concernant les employés apportant leurs propres appareils personnels (BYOD) au laboratoire. Parmi les déclarations suivantes, laquelle est VRAIE?
    A. Une politique BYOD en laboratoire est acceptable, et aucune procédure spécifique n'est nécessaire si les appareils ne sont pas utilisés pour accéder à des informations et des données sensibles du laboratoire.
    B. La politique devrait interdire le BYOD étant donné les défis uniques en matière de cybersécurité, et le niveau de risque plus élevé quand-il s'agit d'environnements de laboratoire manipulant des agents biologiques.
    C. Les procédures de cybersécurité déjà en place pour sécuriser les appareils et les données en laboratoire sont généralement adéquates pour fournir une sécurité efficace également pour le BYOD.
    D. Des politiques et des procédures spécifiques doivent être mises en œuvre pour traiter les risques informatiques uniques liés au BYOD pour l'organisation, ainsi que les risques de confidentialité pour les employés. *

4. L'infrastructure des laboratoires de confinement biologique peut être conçue avec des équipements et des systèmes vulnérables aux cyberattaques.
   Compléter cette déclaration: Lors de la prise en compte de la cybersécurité pour la construction de systèmes de confinement biologique, les responsables des installations devraient _____.
    A. communiquer régulièrement avec leur département informatique et les fournisseurs pour mettre en œuvre des solutions de cybersécurité pour l'infrastructure existante, les contrats de service et de maintenance, ainsi que pour les nouvelles installations*
    B. s'appuyer sur leur département informatique qui possède l'expertise et la responsabilité de développer et d'adopter des politiques et des procédures de cybersécurité pour l'infrastructure de laboratoire et les systèmes de construction
    C. compter sur les fournisseurs qui sont responsables de garantir que leurs systèmes de construction, équipements et personnel de service sont sécurisés contre les vulnérabilités et respectent les meilleures pratiques en matière de cybersécurité
    D. collaborer avec les responsables de laboratoire pour effectuer une analyse de vulnérabilité en cybersécurité et un test de pénétration des systèmes de confinement du bâtiment au moins une fois par mois

5. Complétez cette déclaration: Lors de l'élaboration d'un plan de réponse aux incidents de cybersécurité pour son laboratoire biologique, une organisation devrait _____.
    A. se préparer et élaborer des instructions étape par étape pour que tous les employés puissent gérer chaque incident potentiel qui pourrai avoir un impact négatif sur l'organisation

B. se concentrer sur une préparation générale dans toute l'organisation en mettant davantage l'accent sur la manière de gérer les incidents qui pourraient utiliser des vecteurs d'attaque courants*
C. limiter strictement le partage d'informations sur tous les aspects du plan au sein de l'organisation afin de réduire toutes probabilités d'attaques cybernétiques provenant de menaces internes
D. établir des procédures écrites pour gérer plusieurs incidents sur la base du premier arrivé, premier servi afin de faire gagner du temps aux intervenants en cas d'incident.

Références

En plus de la connaissance des termes de base de la cybersécurité et des fondamentaux, voici quelques suggestions de préparation pour l'examen, qui pourraient inclure, sans s'y limiter, les ressources suivantes:

Assessing Cyberbiosecurity Vulnerabilities and Infrastructure Resilience, Daniel S. Schabacker et al, Frontiers in Bioengineering and Biotechnology, 29 March 2019.

Cyberbiosecurity: A Call for Cooperation in a New Threat Landscape, Lauren C. Richardson et al,
Frontiers in Bioengineering and Biotechnology, 06 June 2019.

Cyberbiosecurity: An Emerging New Discipline to Help Safeguard the Bioeconomy, Randall S. Murch et al, Frontiers in Bioengineering and Biotechnology, 05 April 2018.

Cyberbiosecurity Implications for the Laboratory of the Future, J. Craig Reed & Nicolas Dunaway, Frontiers in Bioengineering and Biotechnology, 21 August 2019.

Cyberbiosecurity: From Naïve Trust to Risk Awareness, Jean Peccoud et al, Trends in Biotechnology, January, 2018.

Cybersecurity Incident Response Exercise Guidance, Larry G. Wlosinski et al, ISACA Journal, Vol 1, January 2022.

Information technology - Security techniques - Guidelines for Cybersecurity, International Standards Organization. ISO/IEC 27032:2012.

Facing the 202 Pandemic: What does Cyberbiosecurity Want us to Know to Safeguard the future? Siguna Meuller, Biosafety & Health, February, 2021.

Computer Security Incident Handling Guide, US National Institute of Standards & Technology NIST, 2012.

Cyberthreats to Biotechnology, US Dept. Health & Human Services, 2021.

Guidelines for Media Sanitation, US National Institute of Standards & Technology, 2014.

Framework for Improving Critical Infrastructure Cybersecurity, US National Institute of Standards & Technology, 2018.

Mobile Device Best Practices, US National Security Agency, 2020.

Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks, US National Institute of Standards & Technology, 2019.