International Federation of Biosafety Associations

Professional Certification in Cyberbiosecurity

Examination Content, Sample Questions & References

The IFBA's Professional Certification (PC) in Cyberbiosecurity identifies individuals with demonstrated competencies in the mitigation of cybersecurity risks within biological laboratories. This includes Information Technology (IT) and Operational Technology (OT) risks in order to protect sensitive biological research, data, databases, and laboratory facilities and equipment against illicit or unauthorized access, theft, tampering, or other forms of misuse.

The PC in Cyberbiosecurity is suited to a wide range of professionals working in and around biological laboratories, biotechnology, pharmaceutical and research laboratories such as biorisk management advisors, biosafety officers, scientific laboratory personnel, biomedical technologists, IT and cybersecurity personnel, facility operations & maintenance personnel, security personnel, management and administration.

For the purposes of this certification, Cyberbiosecurity is defined as "the safeguarding and mitigation of misuse, exploitation, damage to or disruption of valuable information, data, databases, equipment and facilities at the interface of the biological laboratory, related life sciences facilities and digital worlds."

The Body of Knowledge (BOK) below identifies 5 domains (topic areas) and 45 knowledge/task statements that define the competency for certification in Cyberbiosecurity. The content of the examination is based on this BOK and each question on the examination is linked to one of the statements below.

Domain A – Cyberbiosecurity Concepts

1. Describe the emerging field of cyberbiosecurity at the interface between cybersecurity, cyber-physical security, quality management, biosafety and biosecurity.
2. Describe the threats and vulnerabilities associated with cyberbiosecurity across many distinct sectors in the life sciences, biomedical sciences, biotechnology and synthetic biology fields and other aspects of the bioeconomy.
3. Identify ways cyberbiosecurity vulnerabilities in biological laboratories presents a risk to the integrity of biological materials and associated digital data, laboratory workers, the surrounding public community, animals and the environment.
4. Understand how networking devices and equipment compounds vulnerability and cyberbiosecurity risks and how to reduce these risks (e.g., separating less secure devices from network, removing Internet of Things devices that are not critical or secure).

5. Know how to identify, assess, reduce and respond to cyberbiosecurity threats, risks and incidents in biological laboratories associated with their assets with digital components, networked equipment, devices and facility systems.
6. Understand the roles and responsibilities of key cyberbiosecurity personnel (e.g., biosafety officers, laboratory scientists, facility maintenance personnel, IT personnel, administration, security) and the importance of regular communication between them.
7. Know how to develop and implement cyberbiosecurity training programs, foster cyberbiosecurity awareness and good personal cybersecurity practices in the laboratory working environment.
8. Be familiar with and understand how to develop/update organizational policies and Standard Operating Procedures in alignment with relevant cyberbiosecurity best practices.

Domain B – Fundamentals of Cybersecurity

9. Understand the options available to an adversary to conduct physical and cyber surveillance of a facility for objectives that may be subtle, indirect or unexpected, and how to reduce these potential risks.
10. Understand intrusion tactics and techniques that can be used by an adversary to gain access to and exploit data and systems (e.g., social engineering, zero-day exploits, software supply chain compromises, networking, cloud storage, users, email, web applications, remote access portals, mobile devices).
11. Define the terms: Information Technology (IT), Operational Technology (OT) and Internet of Things (IoT).
12. Describe the 3 common categories of multifactor authentication (i.e., knowledge, possession, inherence).
13. Understand the principles of access control (e.g., privacy by design, data protection by design, acceptable use policy, least privileged user accounts, configuring user accounts and security permissions within multiple environments, digital rights management).
14. Understand the principles of identity and access management (e.g., managing entity and group permissions, configuring organizational units and objects).
15. Understand the principles of physical protection (e.g., establishing physical access control) and media protection (e.g., properly sanitizing or destroying media).
16. Understand the principles of system and communications protection (e.g., monitoring external and internal boundary devices, implementation of subnets).
17. Understand the principles of system and information integrity (e.g., identification of system issues, deployment of network/host-based signatures, performance of periodic anti-virus scanning).

Domain C – Information Technology (IT) Risks in Biological Laboratories

18. Describe the different types of data stored and transmitted through information technology platforms and equipment in the biological laboratory that could present a data stream of interest to adversaries.
19. Understand how data vulnerabilities adversely affect quality management through loss of confidentiality (i.e., data loss), loss of availability (i.e., operational disruption) and loss of integrity (i.e., altered data).
20. Describe how exfiltration of data can occur from both an insider and outsider adversary and how database encryption technologies can be used to secure information in biological databases.
21. Describe the ways in which networked laboratory equipment could be remotely/digitally exploited to compromise research integrity, alter genomic sequences, manipulate the characteristics of biological agents, and create harmful biological products.
22. Describe how the use of Demilitarized Zones and Trust Zones can be used to enhance security for networked laboratory equipment and infrastructure.
23. Describe how cryptographic algorithms could be leveraged for password usage, multi-factor authentication, Virtual Private Network, and encryption of data at rest and in transit can be incorporated into a laboratory's cyberbiosecurity policy.
24. Understand the importance of periodic vulnerability assessments and scoped network/application penetration tests that can be leveraged to identify and mitigate vulnerabilities.
25. Know how to reduce cyberbiosecurity vulnerabilities presented by the use of personal devices (e.g., personal laptops and cellphones) to access laboratory-related systems.
26. Understand the vulnerabilities associated with the use of wireless spectrum technologies and equipment connected to the internet, and how wireless devices can increase your attack surface and enable new attack vectors for adversaries.
27. Describe what vulnerabilities and sensitive information can be revealed to adversaries through administrative control documents (e.g., emergency response procedures, safety/security program plans), budget and planning documents, contract documents, floor plans and schematics for laboratories, supporting rooms and mechanical spaces.
28. Describe ways to restrict the disclosure of sensitive information and facility vulnerabilities to outside facility maintenance contractors, equipment service providers and vendors.
29. Understand the cybersecurity vulnerabilities associated with networked pathogen inventory systems and Laboratory Information Management Systems.
30. Know how to identify and mitigate vulnerabilities of laboratory-related activities carried out by personnel that may result in the release of sensitive information (e.g., legitimate data sharing for research, teaching or commercial purposes).

Domain D – Operational Technology (OT) Risks in Biological Laboratories

31. Understand how technological innovation in "smart laboratories" (i.e., laboratories with networked devices capable of remote monitoring and control, smart keys) are subject to cybersecurity vulnerabilities.
32. Understand the cybersecurity vulnerabilities with the use of electronic lab notebooks and voice-driven virtual personal assistant using voice commands in the laboratory.
33. Know how networked building automation systems and energy management software are subject to cybersecurity vulnerabilities.
34. Describe the ways in which a laboratory's physical access control system could be remotely/digitally exploited to compromise security.
35. Describe the ways in which a biocontainment laboratory's building automation system could be remotely/digitally exploited to compromise biosafety, containment, life-safety and the integrity of biological materials/data.
36. Describe the ways in which a biological laboratory's decontamination systems and equipment could be remotely/digitally exploited to compromise biosafety and biocontainment.
37. Describe the ways in which animal housing rooms and containment caging systems could be remotely/digitally exploited and the potential impacts of such an intrusion.
38. Understand the potential cybersecurity risks that may compromise a laboratory's supply chain and how these risks can be minimized and reversed if detected.

Domain E – Preparedness & Response to Cyberbiosecurity Incidents

39. Know how to perform a complete walkthrough of the facility for the purpose of developing a cyberbiosecurity threat mitigation and incident response plan.
40. Describe the development of a comprehensive cyberbiosecurity threat mitigation, incident response and communication plan to minimize damage, contain the threat, and maintain biosafety & biosecurity.
41. Understand the roles and responsibilities of key personnel for responding to cyberbiosecurity incidents both within the organization and from outside specialists.
42. Know in advance where to obtain additional outside trusted and vetted assistance for identifying, responding to and recovering from cyberbiosecurity incidents.
43. Know when and how to involve law enforcement agencies that might be required to respond, investigate, collect probative evidence, and conduct interviews.
44. Know the communication channels, how to report, and to whom, potential and detected cyberbiosecurity incidents.
45. Know how to conduct regular exercises of the cyberbiosecurity incident response team including table-top exercises.

Exam Blueprint

The following represents the number of questions in each domain that are included in the examination:

Exam Blueprint Professional Certification in Cyberbiosecurity Passing Score – 70%	
Domain	**Number of Questions**
A) Cyberbiosecurity Concepts	19
B) Fundamentals of Cybersecurity	18
C) Information Technology (IT) Risks in Biological Laboratories	28
D) Operational Technology (OT) Risks in Biological Laboratories	12
E) Preparedness & Response to Cyberbiosecurity Incidents	13

Sample Questions

In order to familiarize candidates with the nature and form of the examination questions, the following are provided as examples. An asterisk marks the correct answer.

1. Which scenario BEST represents a cyberbiosecurity related concern in today's biological laboratory environment?
   a) Poorly secured laboratories could result in unauthorized individuals gaining access to and stealing pathogens from the laboratory's freezers.
   b) Laboratory equipment and IoT devices connected to the internet could be hacked to access and alter confidential laboratory data.*
   c) Laboratory researchers could sell proprietary scientific information and data to a competing research organization.
   d) Waste materials could be inadequately decontaminated prior to leaving the laboratory for off-site disposal.

2. Complete this statement: Using a _____ to verify a network user's identity is an example of multi-factor authentication to decrease the likelihood of a cyber attack.
   a) password and username
   b) security question and PIN code
   c) one time 4-digit code sent via SMS*
   d) fingerprint scan and facial recognition

3. The IT department is developing a policy and procedures regarding employees bringing their own personal devices (BYOD) into the laboratory. Which statement is TRUE?

a) A laboratory BYOD policy is acceptable, and no specific procedures are required if the devices are not used to access sensitive laboratory information and data.
b) The policy should prohibit BYOD given the unique cybersecurity challenges and a higher level of risk in all laboratory environments handling biological agents.
c) Cybersecurity procedures already in place to secure laboratory devices and data are generally adequate to provide effective security for BYOD as well.
d) Specific policies and procedures need to be implemented that address BYOD's unique IT risks to the organization and privacy risks to employees.*

4. Biological containment laboratory infrastructure may be designed with equipment and systems that are vulnerable to cyber attacks. Complete this statement: When considering cybersecurity and building containment systems, facility managers should _____ .

a) regularly communicate with their IT department and vendors to implement cybersecurity solutions for existing infrastructure, service and maintenance contracts, and new installations*
b) rely on their IT department who have the expertise and responsibility to develop and adopt cybersecurity policies and procedures for laboratory infrastructure and building systems
c) rely on vendors who are liable to ensure their building systems, equipment and service personnel are secure from vulnerabilities and complying with cybersecurity best practices
d) collaborate with laboratory managers to conduct a cybersecurity vulnerability scan and penetration test of the building's containment systems at least once a month

5) Complete this statement: When developing a cybersecurity incident response plan for it's biological laboratory, an organization should _____ .

a) prepare for and develop step-by-step instructions for all employees to handle every potential incident that could negatively impact the organization
b) focus on being generally prepared throughout the organization with a greater emphasis on how to handle incidents that use common attack vectors*
c) strictly limit information sharing about all aspects of the plan within the organization to the reduce the likelihood of cyber attacks from insider threats
d) establish written procedures for handling multiple incidents on a first-come first served basis in order to save time for incident handlers

References

In addition to knowledge of basic cybersecurity terminology and fundamentals, some suggested preparation for examination might include, but should not be limited to, the following resources:

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.