Quizzes

Module 4: Biological Safety, Biological Security, and Biological Weapons

Module 4-1: Biosafety and Biosecurity

1. Match the following

application of knowledge, techniques, and equipment to protect scientific workers, the public, and the environment from accidental exposure to infectious agents and other biohazards	Biosecurity
the safekeeping and prevention of unauthorized access to dangerous pathogens and toxins, as well as microbial strains and biological materials of value	Biosafety

Feedback: Biosafety and biosecurity have different goals; however, they do overlap and complement each other in overall laboratory safety procedures and protective measures.

2. Complete the following:

Biosafety principles guide the conditions for _____; that is, the methods and equipment for safe manipulation of infectious agents in a laboratory.

- Access
- Containment
- Physical protection

Feedback: Access and physical protection are components of containment.

3. **Complete the following:**

   While the goal of biosafety measures is to prevent _____ infection or release of organisms and toxins, biosecurity aims to counter _____ attempts to acquire BW capabilities or materials.

4. **Both biosafety and biosecurity measures seek to minimize risk. When conducting research on pathogenic agents for peaceful purposes, it is necessary to establish what constitutes a(n) _____ level of risk.**

   - acceptable
   - intolerable
   - high

5. **Complete the following with the words:**

   - objective
   - subjective

Assessing risk and determining acceptable risk are _____ because they are based on human judgment. However, *measuring* risk is _____: an analyst determines acceptable risk according to certain standards, using available guidelines, data, and documentation.

6. **Probabilistic risk assessment (PRA) is a systematic and comprehensive methodology to evaluate risks associated with complex technologies such as biotechnologies. In a PRA, risk is characterized by 1) the probability that an adverse event will occur and 2) the severity of the possible adverse outcomes. With this in mind, complete the following:**

To determine acceptable risk, medical professionals must consider and plan for the worst-case scenario. They must estimate the _____ of different types of negative incidents occurring, along with the seriousness and likely _____ of such incidents. Then, they must determine what _____ to take to respond to and resolve an incident.

7. **Complete the following:**

The level of risk posed by a biological agent depends on the biology of the agent, as well as how it is _____ to *and* _____ the hosts.

8. Complete the sentence with one of the pairs below.

When identifying risk and addressing hazards, the goal is to provide the highest practical _____ and the lowest practical _____.

- resistance / virulence
- attenuation / pathogenicity
- protection / exposure

9. The World Health Organization (WHO) has a system for classifying biological agents based on the risks that they pose. Match the descriptions to the appropriate risk group level (1-4).

Agents that are unlikely to cause disease and therefore pose low levels of individual and community risk	4
Agents that cause serious or fatal disease that often are not treatable; often are contagious	3
Agents that typically cause respiratory infections that cause serious diseases, although they are usually treatable	2
Agents that cause diseases, but these typically are not serious and treatments are available	1

10. The WHO has a system that depends on biosafety levels (BSLs) for managing dangerous pathogens. Match the biosafety level to its description.

Work with high-risk agents that can spread through aerosol transmission and often contagious; can cause serious or lethal disease; controlled, negative pressure environment; access to the lab restricted only to authorized individuals	BSL-1
Work with high-risk, highly transmissible and potentially lethal agents; no vaccines or treatments available; labs airtight with containment measures including "submarine" doors, air pumps, negative pressure, and HEPA filtration; workers must wear positive pressure suits	BSL-2
Work with risk group 1 agents without containment measures; need to follow good laboratory practices, proper waste disposal, and aseptic techniques	BSL-3
Work with agents that pose moderate hazards; lab should be restricted and containment procedures used during certain processes; use of biological safety cabinets, fume hoods, and autoclaves	BSL-4

11. Complete the following:

BSLs are quite different than Risk Groups. Risk Groups are used to conduct _____ of risks posed by different kinds of agents, while BSLs define the _____ under which every pathogen is to be handled in the laboratory or transported from site to site. BSLs thus structure the procedures and measures necessary to prevent agents from infecting workers and communities.

Module 4- 2: Acquiring a Biological Weapon Capability

1. **Similar to chemical weapons, biological weapons are multi-component systems. Match the components to their descriptions:**

the active ingredient of the system	Dispersal device
chemical mixed with pathogens; may be "wet" or "dry"	Pathogen
protects the formulated pathogen during transport and storage	Munition
usually sprayer or atomizer for creating aerosol	Formulation

2. **Complete the following**

   The acquisition of a biological weapons capability has three main requirements. First, it is necessary to have skilled _____ to weaponize biological agents. Next, a dangerous pathogen or _____ is needed. Finally, special _____ is needed to disperse biological weapons agents over a targeted population. Biosecurity measures are successful if they prevent a proliferant nation or terrorist group from acquiring any one or more of these three requirements.

3. **Which of the following are considered ideal biological weapons agents and subject to biosecurity measures?**

   Bacillus anthracis (anthrax)
   Botulinum (botulism)
   Bordetella pertussis (pertussis)
   Yersinia pestis (plague)
   Variola major (smallpox)
   Vibrio cholerae. (cholera)
   Francisella tularensis (tularemia)
   Ebola virus (Ebola hemorrhagic fever)
   Escherichia coli (salmonella)
   Clostridium tetani (tetanus)

4. **Choose the best option for the blank in this sentence:**

   The special equipment needed for a biological weapons capability is _____, being also widely employed in industry and science, and is therefore difficult to regulate and control.

   - dual use
   - technical
   - weaponized

5. **Which of the following are the *most likely* ways that terrorists could acquire biological agents?**

   - genetically engineer an agent
   - burglarize low-security laboratories
   - steal a high-level agent such as smallpox
   - acquire select agents such as anthrax from natural sources
   - collaborate with a laboratory employee

6. **Which of the following would be *relatively easy* for terrorists to acquire?**

   - agar and growth media
   - equipment to grow and process pathogens for dispersal
   - explosive dispersal devices
   - gas masks and other personal protective equipment
   - dispersal devices such as sprayers

7. **Place the following in order from *easiest* to *most difficult*:**

   - disperse an aerosolized bacteria or toxin
   - sabotage the food industry with a pathogen or toxin
   - contaminate food or beverages with pathogens or toxins
   - disperse an aerosolized virus

8. **Which of the following is considered a very worrisome bioweapon because it is easy to acquire, easy to work with, and highly toxic?**

   - Anthrax
   - Botulinum toxin
   - Ricin

Module 4-3: Violation of Biosecurity by Terrorists – Two Case Studies

1. This part of the module considers two case studies of terrorist use of biological agents. The first case involves the Rajneeshee cult and the second to Aum Shinrikyo. Match the description to the appropriate terrorist group.

use of a foodborne bacteria, *Salmonella typhimurium*	Aum Shinrikyo
Aerosolized biological attack using *Bacillus anthracis*	Rajneeshees

2. What was the Rajneeshees' motivation to use biological weapons in a rural area of the United States?

- To affect the outcome of a local election in their favor
- To kill local citizens who spoke out against them
- To prevent government officials from inspecting their land

3. Which of the following are reasons that the Rajneeshee case is an example of "a relatively low level of skill attempting the easiest level of biological acquisition and dispersal"?

- The group could legitimately receive cultures of dangerous organisms
- They cultured a high-level infectious agent
- They invested heavily in sprayers and other equipment
- The bacteria were dispersed using a spray bottle
- Their attempts did not have the intended effect

4. What was Aum Shinrikyo's motivation for using chemical and biological weapons in Tokyo?

- To gain power by taking over the government
- To gain legitimacy by triggering a nuclear apocalypse
- To gain large sums of money by selling its weapon capability

5. Complete the sentence with one of the choices below.

The Aum Shinrikyo cult used a(n) _____to disperse *Bacillus anthracis* from the roof of an eight-story building that it owned.

- Explosive munition
- Aerosol system
- Gravity bomb

6. Which of the following are among the lessons learned from the Aum Shinrikyo and Rajneeshee cases?

- It is quite possible for terrorist groups to use highly pathogenic organisms to cause mass casualties
- A high level of education and money does not guarantee success
- A low level of education and skill does not guarantee failure
- Many things can go wrong, such as obtaining the wrong strain or having problems with equipment
- The goal of securing and controlling the distribution of biological materials is highly important

Module 4-4: Methods of Preventing Breaches of Biosecurity in Vital Bioscientific Facilities

1. **Accomplishing biosecurity involves a cost-benefit consideration because it is _____ to perfectly secure every aspect of a facility and its assets.**
   - essential
   - impossible
   - hazardous

2. **According to the video, establishing a biosecurity methodology involves a series of steps. Put them in the correct order:**
   - A rational decision to take measures
   - Identification of adversaries and assessment of their capabilities
   - Identification and evaluation of various scenarios for unauthorized access to facilities
   - A qualitative risk and threat assessment
   - Identification and prioritization of assets according to probability and consequences

3. **Match the scenarios with the appropriate adversary category.**

A highly trained microbiologist in a BSL-3 laboratory secretly removes bacillus anthracis spores from the lab	Invited outsider(s) – visitor
A highly trained microbiologist who is secretly working for a competing company is invited to work at the lab and removes information from a computer	Insider with authorized access
An animal rights group breaks through the outer parameter of a biological facility and defaces the buildings with graffiti	Collusion between an insider and an outsider
A terrorist or criminal pays an employee at a laboratory to steal an access card to the facility	Outsider(s) with no access but has general knowledge

4. Match the scenarios to the appropriate level of risk.

Insider or outsider attempts to steal information	Lowest risk
Terrorist commando assault	Medium risk
Insider or outsider attempts to steal select agents	High risk
Small outsider groups attack facility	Highest risk

5. Match biosecurity protection principles to their descriptions.

Background investigations on individuals who handle, use, or transfer select agents; screen and escort visitors	Program Management
Detectors, access controls, alarm systems, barriers, guards and law enforcement	Material Control and Accountability
Systems to monitor and document materials in a facility, where they are located, who is responsible for them, who has access to them	Personnel Reliability
Document, account for, and control agents moving between protected areas within a facility and between registered facilities	Material Transfer Security
Control access to sensitive information whether paper-based, telephonic, photographic, or electronic media	Physical Security
Oversee implementation of biosecurity program: security plan, incident response plan, training program, self-assessment and auditing	Information Technology Security

Answers

Module 4-1: Biosafety and Biosecurity

1. Biosafety → application of knowledge, techniques, and equipment to protect scientific workers, the public, and the environment from accidental exposure to infectious agents and other biohazards

   Biosecurity → the safekeeping and prevention of unauthorized access to dangerous pathogens and toxins, as well as microbial strains and biological materials of value

2. Containment✓

3. While the goal of biosafety measures is to prevent accidental infection or release of organisms and toxins, biosecurity aims to counter deliberate attempts to acquire BW capabilities or materials.

4. acceptable✓

5. Assessing risk and determining acceptable risk are subjective because they are based on human judgment. However, *measuring* risk is objective: an analyst determines acceptable risk according to certain standards, using available guidelines, data, and documentation.

6. To determine acceptable risk, medical professionals must consider and plan for the worst-case scenario. They must estimate the likelihood of different types of negative incidents occurring, along with the seriousness and likely consequences of such incidents. Then, they must determine what measures to take to respond to and resolve an incident.

7. The level of risk posed by a biological agent depends on the biology of the agent, as well as how it is transmitted to *and* affects the hosts.

8. protection / exposure✓

9.

4	→	Agents that cause serious or fatal disease that often are not treatable; often are contagious
3	→	Agents that typically cause respiratory infections that cause serious diseases, although they are usually treatable
2	→	Agents that cause diseases, but these typically are not serious and treatments are available
1	→	Agents that are unlikely to cause disease and therefore pose low levels of individual and community risk

10.

BSL-1	→	work with risk group 1 agents without containment measures; need to follow good laboratory practices, proper waste disposal, and aseptic techniques
BSL-2	→	Work with agents that pose moderate hazards; lab should be restricted and containment procedures used during certain processes; use of biological safety cabinets, fume hoods, and autoclaves
BSL-3	→	Work with high-risk agents that can spread through aerosol transmission and often contagious; can cause serious or lethal disease; controlled, negative pressure environment; access to the lab restricted only to authorized individuals
BSL-4	→	Work with high-risk, highly transmissible and potentially lethal agents; no vaccines or treatments available; labs airtight with containment measures including "submarine" doors, air pumps, negative pressure, and HEPA filtration; workers must wear positive pressure suits

11. BSLs are quite different than Risk Groups. Risk Groups are used to conduct <u>assessments</u> of risks posed by different kinds of agents, while BSLs define the <u>conditions</u> under which every pathogen is to be handled in the laboratory or transported from site to site. BSLs thus structure the procedures and measures necessary to prevent agents from infecting workers and communities.

Module 4- 2: Acquiring a Biological Weapon Capability

1. Pathogen → the active ingredient of the system

   Formulation → chemical mixed with pathogens; may be "wet" or "dry"

   Munition → protects the formulated pathogen during transport and storage

   Dispersal device → usually sprayer or atomizer for creating aerosol

2. The acquisition of a biological weapons capability has three main requirements. First, it is necessary to have skilled people to weaponize biological agents. Next, a dangerous pathogen or toxin is needed. Finally, special equipment is needed to disperse biological weapons agents over a targeted population. Biosecurity measures are successful if they prevent a proliferant nation or terrorist group from acquiring any one or more of these three requirements.

3.

- Bacillus anthracis (anthrax) ✓
- Botulinum (botulism) ✓
- Yersinia pestis (plague) ✓
- Variola major (smallpox) ✓
- Francisella tularensis (tularemia) ✓
- Ebola virus (Ebola hemorrhagic fever) ✓

4. dual use✓

5.

- burglarize low-security laboratories ✓
- acquire select agents such as anthrax from natural sources✓
- collaborate with a laboratory employee ✓

6.

- agar and growth media ✓
- equipment to grow and process pathogens for dispersal ✓
- gas masks and other personal protective equipment ✓
- dispersal devices such as sprayers ✓

7.

- contaminate food or beverages with pathogens or toxins (1)
- sabotage the food industry with a pathogen or toxin (2)
- disperse an aerosolized bacteria or toxin (3)
- disperse an aerosolized virus (4)

8. Ricin✓

Module 4-3: Violation of Biosecurity by Terrorists – Two Case Studies

1. Rajneeshees → use of a foodborne bacteria, Salmonella typhimurium

   Aum Shinrikyo → Aerosolized biological attack using Bacillus anthracis

2. To affect the outcome of a local election in their favor✓

3.
   - The group could legitimately receive cultures of dangerous organisms ✓
   - The bacteria were dispersed using a spray bottle ✓
   - Their attempts did not have the intended effect✓

4. To gain legitimacy by triggering a nuclear apocalypse✓

5. Aerosol system✓

6. Which of the following are among the lessons learned from the Aum Shinrikyo and Rajneeshee cases?

   - It is quite possible for terrorist groups to use highly pathogenic organisms to cause mass casualties✓
   - A high level of education and money does not guarantee success✓
   - A low level of education and skill does not guarantee failure✓
   - Many things can go wrong, such as obtaining the wrong strain or having problems with equipment✓
   - The goal of securing and controlling the distribution of biological materials is highly important✓

Module 4-4: Methods of Preventing Breaches of Biosecurity in Vital Bioscientific Facilities

1. impossible✓

2.
   - A qualitative risk and threat assessment (1)
   - Identification and prioritization of assets according to probability and consequences (2)
   - Identification of adversaries and assessment of their capabilities (3)
   - Identification and evaluation of various scenarios for unauthorized access to facilities (4)
   - A rational decision to take measures (5)

3.

Insider with authorized access	→	A highly trained microbiologist in a BSL-3 laboratory secretly removes bacillus anthracis spores from the lab
Invited outsider(s) – visitor	→	A highly trained microbiologist who is secretly working for a competing company is invited to work at the lab and removes information from a computer
Outsider(s) with no access but has general knowledge	→	An animal rights group breaks through the outer parameter of a biological facility and defaces the buildings with graffiti
Collusion between an insider and an outsider	→	A terrorist or criminal pays an employee at a laboratory to steal an access card to the facility

4. Match the scenarios to the appropriate level of risk.

Lowest risk	→	Terrorist commando assault
Medium risk	→	Small outsider groups attack facility
High risk	→	Insider or outsider attempts to steal information
Highest risk	→	Insider or outsider attempts to steal select agents

5.

Personnel Reliability	→	Background investigations on individuals who handle, use, or transfer select agents; screen and escort visitors
Physical Security	→	Detectors, access controls, alarm systems, barriers, guards and law enforcement
Material Control and Accountability	→	Systems to monitor and document materials in a facility, where they are located, who is responsible for them, who has access to them
Material Transfer Security	→	Document, account for, and control agents moving between protected areas within a facility and between registered facilities
Information Technology Security	→	Control access to sensitive information whether paper-based, telephonic, photographic, or electronic media
Program Management	→	Oversee implementation of biosecurity program: security plan, incident response plan, training program, self-assessment and auditing