APHL ASSOCIATION OF PUBLIC HEALTH LABORATORIES®

MAY 2025

Laboratory Biosecurity Risk Assessment Tool

A Guide for Public Health and Clinical Diagnostic Laboratories

The Association of Public Health Laboratories' (APHL) Laboratory Biosecurity Risk Assessment Tool is intended to assist public health and clinical laboratories in evaluating potential biosecurity threats and vulnerabilities related to their biological materials, equipment, personnel and operations. By providing concise guidance and a structured method, this tool helps laboratories identify, prioritize and mitigate biosecurity risks to enhance protective measures and strengthen biosecurity programs. Download an editable version of this Tool to work through these steps within your laboratory.

Background

Conducting a laboratory biosecurity risk assessment is essential for the biosecurity of public health and clinical diagnostic labs. It enables leaders to better recognize specific risks and provide support for effective biosecurity programs. A thorough biosecurity risk assessment identifies valuable laboratory assets, evaluates the probability and consequences of each threat scenario, considers information about known vulnerabilities and assesses the overall biosecurity risk to the laboratory—allowing leaders to allocate resources efficiently. The results provide laboratory leaders with a list of potential biosecurity scenarios, identified vulnerabilities and proposed mitigation measures. Additionally, risk assessments provide a framework to design custom biosecurity drills and evaluate staff competencies.

This tool is designed to adapt to the needs of individual laboratories. Rather than conducting a comprehensive threat and vulnerability assessment, which may be extensive, laboratories can concentrate on specific programs, assets or categories of risk. For instance, this tool can be applied to areas such as:

- Biological inventories and high-consequence pathogens
- Critical infrastructure, like laboratory ventilation or data systems (e.g., laboratory information management system [LIMS])
- Known threat actors (e.g., insider and outsider threats)
- Access control and physical security, including visitor management, badge access and restricted areas

By performing smaller, focused assessments, laboratories can integrate biosecurity into their operations and ensure a practical and sustainable process for improving the laboratory biosecurity program. Like biosafety risk assessments, laboratory biosecurity risk assessments should be living documents and require routine, periodic reviews and updating whenever there is an impactful change to any piece of the previous assessment.

Contents

Conducting a Laboratory Biosecurity Risk Assessment

A laboratory biosecurity risk assessment encompasses several key components designed to systematically identify and evaluate the factors contributing to biosecurity risks faced by laboratories. This assessment is best conducted by a multidisciplinary team to ensure varied expertise and perspectives, including members from relevant disciplines, such as scientists, biosafety and biosecurity professionals, information technology personnel, facility operations and laboratory managers.

The chosen experts should possess extensive knowledge of the laboratory's assets, processes and operations, and be well-versed in industry best practices for laboratory biosecurity and relevant regulatory requirements. Additionally, involving security and threat assessment professionals with experience in identifying vulnerabilities, mitigating security risks and assessing threats specific to the relevant industry or geographical area is helpful.

If internal security and threat assessment resources are limited or unavailable, local law enforcement agencies can provide support either through direct involvement or by facilitating connections to other resources.

Once assembled, the team should collaboratively address the main elements of the laboratory biosecurity risk assessment, including:

- Identifying valuable laboratory assets that require protection
- Assessing threats from both authorized insiders and malicious outsiders
- Evaluating vulnerabilities within the existing biosecurity program
- Recommending mitigation measures to reduce overall biosecurity risks

The following sections walk through the biosecurity risk assessment process. For simplicity, this document provides a single example of an asset, threat and vulnerability. However, when completing a site-specific biosecurity assessment, these steps must be repeated for each asset, threat and vulnerability identified.

Security and Confidentiality Notice

Information documented in a laboratory biosecurity risk assessment should be managed securely and confidentially. Due to the sensitive nature of identifying laboratory assets, threats and vulnerabilities, access to any completed biosecurity risk assessment should be strictly limited to authorized parties. Laboratories conducting these biosecurity risk assessments are encouraged to coordinate with their local law enforcement agencies or other security professionals to ensure proper management and to access additional resources for strengthening biosecurity measures.

Step One: Identify Valuable Assets

An essential preliminary step in a laboratory biosecurity risk assessment is to compile an inventory of the relevant valuable assets within the laboratory, clearly identifying the items requiring protection. Valuable laboratory assets include items vital to daily operations, whose security is paramount for maintaining public trust and fulfilling the laboratory's mission. Regularly reviewing and updating the laboratory asset inventory helps maintain an accurate assessment that adapts to evolving laboratory operations and emerging threats.

Determining the value of an asset involves more than just assessing its replacement or repair cost. It is also essential to evaluate the consequences of an asset being lost, stolen, compromised or rendered dysfunctional. Additionally, consideration should be given to the impact on laboratory operations, business and financial functions, customer/client relations, public health and safety, and the overarching mission of the laboratory. Following an assessment, each asset should be assigned a priority or value level. For simplicity, a "low/medium/high" ranking has been used here to assign value to assets; if needed, a more complex approach, such as an alphabetical or numerical ranking system, may also be utilized.

Examples of Assets

Valuable assets may include:

Materials and Data

- Test samples
- Material inventories
- Reagents
- Laboratory data
- Sensitive patient, personnel or laboratory information
- Intellectual property

Facilities and Operational Systems

- Laboratory equipment
- Financial systems
- Information technology
- Building management systems

Example: Asset Identification

In this section, we will use an inventoried biological asset to demonstrate the asset identification and valuation process. Each laboratory should follow the same steps for each asset identified in its site-specific assessment.

Asset Name or Description	Impact of Loss or Compromise	Value/Priority Level
Inventoried biological agent Example: Risk Group 3 human pathogen, such as *Mycobacterium tuberculosis*, *Brucella abortus, Coccidioides immitis*, SARS-CoV/SARS-CoV2, Hendra Virus, Middle East Respiratory Syndrome Coronavirus, Yellow Fever Virus, Chikungunya Virus, and/or Hantavirus	Theft or loss could result in a threat to public health and safety, legal and regulatory consequences, damaged public confidence, and possible loss of accreditation or registration to perform work.	**High**

Step Two: Classify Threats

Biosecurity threats encompass any malicious intentions and actions that can cause adverse events, such as injury, disruption, damage, theft, diversion, misuse, unauthorized access, intentional release of materials or information, or sabotage.[1] These threats may be identified from current events, past incidents, industry-specific information, and local or regional intelligence about individuals or groups with potential motives to target laboratory facilities. While external threats from people or groups outside the laboratory are often considered, insider threats should not be overlooked. Authorized personnel have legitimate access to valuable laboratory assets and the technical knowledge and expertise required by many malicious plots. For these reasons, maligned insiders are often deemed the greatest threat by laboratory biosecurity programs.

Classifying threats involves assessing both the **likelihood** of an attack on the laboratory and the severity of the **consequences** if such an event were to occur. A threat assessment matrix can be employed to determine the overall threat classification level based on these considerations. While various ranking systems can be utilized, a "low/medium/high" classification has been applied here to rank likelihood, consequence and overall threat level.

Figure 1: Likelihood Versus Consequence Matrix

This matrix illustrates a basic methodology for assessing a threat level by determining the consequence of a successful biosecurity attack and the likelihood that the biosecurity attack will be carried out. The point of intersection between likelihood and consequence determines the overall threat level.

		Consequence		
		Low	Medium	High
Likelihood	Low	Low	Low	Medium
	Medium	Low	Medium	High
	High	Medium	High	High

Example: Threat Assessment

Using **Figure 1**, determine consequence and likelihood of an attack to establish a **Threat Level (T1)**. Repeat this process for each identified asset, ensuring consistent evaluation of threat levels.

Threat Name or Description	Consequence of Attack	Likelihood of Attack	Threat Level (T1)
Disgruntled employee (insider threat)	**High**	**Medium**	**High**

1 Laboratory Biosecurity Guidance, World Health Organization (2024)

Step Three: Evaluate Vulnerabilities

Despite existing control measures, biosecurity vulnerabilities often remain. Identifying these vulnerabilities can be achieved through personnel discussions, self-assessment of policies and procedures, external biosecurity program reviews, and an active training and exercising program. Drills and exercises are particularly effective as they highlight strengths and weaknesses in both policies and procedures while also testing staff competency levels. This approach not only helps to identify biosecurity vulnerabilities but also enhances biosecurity training programs. The APHL Biosecurity Exercises Toolkit for Public Health and Clinical Diagnostic Laboratories serves as a helpful resource for designing and conducting biosecurity drills and exercises.

Once a vulnerability is identified, it is important to determine its cause and assign a vulnerability level (i.e., low, medium or high) to help assess its impact on the security of any associated valuable laboratory assets.

Figure 2: Vulnerability Level Descriptions

The table below provides basic definitions for low, medium and high-level biosecurity vulnerabilities.

Vulnerability Level	A vulnerability which, if exploited…
Low	Is unlikely to independently enable a successful biosecurity attack.
Medium	May independently enable a successful biosecurity attack.
High	Will almost certainly enable a successful biosecurity attack.

Example: Vulnerability Assessment

Identify vulnerabilities that could be exploited to allow threats identified in **Step Two** to be carried out successfully. Determine the cause of vulnerability and assign a **vulnerability level (V1)** based on its level of impact.

Vulnerability Name or Description	Cause of Vulnerability	Vulnerability Level (V1)
Lack of suitability program	No requirement for a suitability program because there is no Tier 1 Select Agent Program at this laboratory.	**Medium:** Lack of a suitability program may enable a threat actor to execute an attack. However, concerning behavior could still be noticed and reported even without a formal program in place.

Step Four: Assess Biosecurity Risk

Laboratory biosecurity risk encompasses the threats directed at the laboratory (**Step Two**) as well as the existing biosecurity vulnerabilities (**Step Three**). After identifying these elements, the overall biosecurity risk can be evaluated using a matrix that compares threat against vulnerability. Given the often-limited resources for enhancing biosecurity, the assessed risk level can be used to prioritize risks, ensuring that finite resources are allocated effectively. Furthermore, the value assigned to the relevant assets must also be considered, as it is essential to secure high-value assets, even if their risk level is lower compared to other assets.

Figure 3: Threat Versus Vulnerability Matrix

This matrix illustrates a basic methodology for assessing a biosecurity risk level based on the threat and vulnerability levels defined in **Figure 1 (page 4)** and **Figure 2 (page 5)**.

		Vulnerability (V1)		
		Low	Medium	High
Threat (T1)	Low	Low	Low	Medium
	Medium	Low	Medium	High
	High	Medium	High	High

Example: Biosecurity Risk Assessment (T1 x V1)

Using **Figure 3**, determine the initial risk level by the identified initial threat and vulnerability levels.

Threat Name or Description	Initial Threat Level (T1)	Vulnerability Name or Description	Initial Vulnerability Level (V1)	Initial Risk Level (T1 x V1)
Disgruntled employee (insider threat)	High	Lack of suitability program	Medium	High

Step Five: Mitigate the Risk

Once the laboratory biosecurity risk has been fully assessed, it is essential to determine how the risk level compares to the laboratory's risk tolerance. If there is a need to reduce risk, effective mitigation strategies must aim to lower one or more of the following: asset value, threat consequence, threat likelihood or vulnerability. While reduction in any of these areas may be possible, addressing vulnerabilities often represents the most practical and effective approach. Identified controls must be actively implemented to enhance existing security measures or new ones introduced to address recognized vulnerabilities. Furthermore, mitigation strategies should be regularly updated based on new findings from ongoing assessments and emerging threats to ensure ongoing effectiveness and continuous improvement.

Example: Mitigation

Once an initial risk is assessed, identify risk mitigation strategies and determine a **residual threat** (**T2**), **vulnerability** (**V2**) and **risk level** (**T2 x V2**) with the new mitigation strategies in place (refer to **Step Two**, **Step Three** and **Step Four**).

Initial Risk Level (T1 x V1)	Risk Mitigation Strategy(s)	Residual Threat Level (T2)	Residual Vulnerability Level (V2)	Residual Risk Level (T2 x V2)
High	• Create an institutional policy for establishing a suitability program. • Provide behavioral threat assessment training to personnel. • Work with human resources to ensure personnel exhibiting concerning behaviors are identified and effective management techniques are employed. • Coordinate with Security and IT to modify access and privileges, if necessary.	**Medium**	**Low**	**Low**

Conclusion

The Laboratory Biosecurity Risk Assessment Tool provides a structured approach for public health and clinical diagnostic laboratories to identify, evaluate and mitigate biosecurity risks. By assessing assets, threats and vulnerabilities, laboratories can effectively prioritize resources, strengthen security measures and better integrate biosecurity into routine operations.

This tool not only enhances laboratory preparedness but also supports compliance with biosecurity best practices and relevant regulatory requirements. Regularly reviewing and updating biosecurity risk assessments ensures laboratories remain resilient in the face of evolving threats, which protects public health and laboratory integrity.

Appendix: Biosecurity Risk Assessment Examples

The following scenarios walk through the biosecurity risk assessment process, using realistic but fictional information. The information contained here should be used for example purposes only.

For simplicity, Scenarios A and B use a single example of an asset (asset number 001); in a real site-specific biosecurity assessment, these steps must be repeated for each asset, threat and vulnerability identified.

Asset Identification Table

Asset #	Asset Name or Description	Impact of Asset Loss/Compromise	Asset Value or Priority Level
001	**Inventoried biological agent** Example: Risk Group 3 human pathogen, such as *Mycobacterium tuberculosis*, *Brucella abortus, Coccidioides immitis*, SARS-CoV/SARS-CoV2, Hendra Virus, Middle East Respiratory Syndrome Coronavirus, Yellow Fever Virus, Chikungunya Virus and/or Hantavirus)	Theft or loss could result in a threat to public health and safety, legal and regulatory consequences, damaged public confidence, and possible loss of accreditation or registration to perform work.	**High**
002	**Sequencing instrument connected to the laboratory network and the LIMS**	If a sequencing instrument was unknowingly compromised but remained functional, there could be impacts to test results, patient health outcomes, protected health information, public health surveillance and public confidence. If the instrument was compromised through a cyberattack, there could be persistent, lateral attacks and impacts on additional assets.	**High**
003	**Sequencing instrument**	If one sequencing instrument was physically damaged or otherwise rendered inoperable there could be financial impacts for repair or replacement and potential impacts to testing capacity or turnaround time. However, samples could be tested on redundant instruments in the lab.	**Medium**
004	**Heating, ventilation and air conditioning (HVAC) controls for a biosafety level 2 (BSL-2) serology laboratory**	Compromised or non-operational HVAC controls may result in poor air ventilation, heating and air conditioning in the laboratory leading to intolerable working conditions and financial impacts for repair or replacement. However, BSL-2 laboratories handle biological agents associated with moderate human disease and all procedures that may create infectious aerosols are performed in a biosafety cabinet or other physical containment equipment. While a good design, inward directional airflow is not a requirement for BSL-2 laboratories. Additionally, most serology specimens do not contain high concentrations of infectious agents.	**Low**

Scenario A: Disgruntled Employee

For one laboratory asset identified in the Asset Identification Table above, assess known threats and vulnerabilities, and the overall biosecurity risk.

Step A One: Asset Identification

Asset #	Asset Name or Description	Impact of Asset Loss/Compromise	Asset Value or Priority Level
001	**Inventoried biological agent** Example: Risk Group 3 human pathogen, such as *Mycobacterium tuberculosis*, *Brucella abortus, Coccidioides immitis*, SARS-CoV/SARS-CoV2, Hendra Virus, Middle East Respiratory Syndrome Coronavirus, Yellow Fever Virus, Chikungunya Virus and/or Hantavirus)	Theft or loss could result in a threat to public health and safety, legal and regulatory consequences, damaged public confidence, and possible loss of accreditation or registration to perform work.	**High**

Step A Two: Classify Threats

Using **Figure 1 (page 4)**, determine the consequence and likelihood of an attack to establish a **threat level** (**T1**). Repeat this process for each identified asset, ensuring consistent evaluation of threat levels.

Asset #	Threat Name or Description	Consequence of Attack	Likelihood of Attack	Threat Level (T1)
001.1	**Disgruntled employee (insider threat)**	**High**	**Low**	**Medium**

Step A Three: Evaluate Vulnerabilities

Identify vulnerabilities that could be exploited to allow threats identified in **Step Two** to be carried out successfully. Determine the cause of vulnerability and, using **Figure 2 (page 5)**, assign a **vulnerability level** (**V1**).

Vulnerability Name or Description	Cause of Vulnerability	Vulnerability Level (V1)
Poor inventory management practices	No strict policy for inventory management at this laboratory. Also, there is no formal training or inventory management system.	**Low:** A vulnerability which, if exploited, is unlikely to independently enable a successful biosecurity attack.

Step A Four: Assess Biosecurity Risk

Using **Figure 3 (page 6)**, determine the initial risk level by the identified initial threat and vulnerability levels.

Threat Name or Description	Initial Threat Level (T1)	Vulnerability Name or Description	Initial Vulnerability Level (V1)	Initial Risk Level (T1 x V1)
Disgruntled employee (insider threat)	**Medium**	**Poor inventory management practices**	**Low**	**Low**

Step A Five: Mitigation

Once an initial risk is assessed, identify risk mitigation strategies and determine a **residual threat (T2)**, **vulnerability (V2)** and **risk level (T2 x V2)** with the new mitigation strategies in place (refer to Step A Two, Step A Three and Step A Four).

Asset #	Unmitigated	Mitigation	Mitigated		
	Initial Risk Level (T1xV1)	Risk Mitigation Strategy(s)	Residual Threat Level (T2)	Residual Vulnerability Level (V2)	Residual Risk Level (T2xV2)
001.1	Low	• Create an inventory management policy and procedure. • Create or procure an inventory management system. • Provide inventory management training.	Medium	Low	Low

Scenario B: Extremist Group

For one laboratory asset identified in the Asset Identification Table above, assess known threats and vulnerabilities, and the overall biosecurity risk.

Step B One: Asset Identification

Asset #	Asset Name or Description	Impact of Asset Loss/Compromise	Asset Value or Priority Level
001	**Inventoried biological agent** Example: Risk Group 3 human pathogen, such as *Mycobacterium tuberculosis*, *Brucella abortus, Coccidioides immitis*, SARS-CoV/SARS-CoV2, Hendra Virus, Middle East Respiratory Syndrome Coronavirus, Yellow Fever Virus, Chikungunya Virus and/or Hantavirus)	Theft or loss could result in a threat to public health and safety, legal and regulatory consequences, damaged public confidence, and possible loss of accreditation or registration to perform work.	High

Step B Two: Classify Threats

Using Figure 1 (page 4), determine the consequence and likelihood of an attack to establish a **threat level (T1)**. Repeat this process for each identified asset, ensuring consistent evaluation of threat levels.

Asset #	Threat Name or Description	Consequence of Attack	Likelihood of Attack	Threat Level (T1)
001.2	**Extremist group (outsider threat) with motivations against healthcare and public health facilities and known activity in the region**	High	High	High

Step B Three: Evaluate Vulnerabilities

Identify vulnerabilities that could be exploited to allow threats identified in **Step Two** to be carried out successfully. Determine the cause of vulnerability and, using Figure 2 (page 5), assign a **vulnerability level (V1) based on its level of impact.**.

Vulnerability Name or Description	Cause of Vulnerability	Vulnerability Level (V1)
Inoperable security cameras	Current cameras are inoperable and unrepairable and there are currently no funds for replacement cameras.	**High:** A vulnerability which, if exploited, will almost certainly enable a successful biosecurity attack.

Step B Four: Assess Biosecurity Risk

Using Figure 3 (page 6), determine the initial risk level by the identified initial threat and vulnerability levels.

Threat Name or Description	Initial Threat Level (T1)	Vulnerability Name or Description	Initial Vulnerability Level (V1)	Initial Risk Level (T1 x V1)
Extremist group (outsider threat) with motivations against healthcare and public health facilities and known activity in the region	**High**	**Inoperable security cameras**	**High**	**High**

Step B Five: Mitigation

Once an initial risk is assessed, identify risk mitigation strategies and determine a **residual threat (T2)**, **vulnerability (V2)** and **risk level (T2 x V2)** with the new mitigation strategies in place (refer to Step B Two, Step B Three and Step B Three).

Asset #	Unmitigated	Mitigation	Mitigated		
	Initial Risk Level (T1xV1)	Risk Mitigation Strategy(s)	Residual Threat Level (T2)	Residual Vulnerability Level (V2)	Residual Risk Level (T2xV2)
001.2	**High**	• Advocate to laboratory administration the importance of prioritizing funds to replace the security cameras. • Minimize the number of accessible laboratory entry points. • Position security guards at accessible laboratory entry points.	**High**	**Low**	**Medium**

Definitions

- **Asset (laboratory):** Any item, resource or information of value to an organization that is essential to its operations, mission or security, or supports its overall function. This includes biological materials, sensitive data, equipment, personnel or infrastructure.
- **Consequence (of a successful biosecurity attack):** The outcome or impact of a successful biosecurity attack occurring in the laboratory.
- **Laboratory biosecurity:** Measures that are taken to safeguard sensitive biological materials and information against theft, loss, misuse, diversion or intentional release.
- **Likelihood (of a biosecurity attack):** The possibility that or frequency with which a specific threat actor would carry out an attack.
- **Mitigation:** The actions, strategies or measures implemented to reduce the likelihood, impact or consequences of a risk or threat. In the context of biosecurity, mitigation focuses on strengthening vulnerabilities, enhancing protective measures and minimizing potential harm to assets, operations and public safety.
- **Risk (biosecurity):** The potential for people (i.e., threats) carry out targeted attacks on laboratory assets. Risk is a function of both the likelihood of a biosecurity attack being carried out and the expected consequences of a successful attack.
- **Threat:** A malicious intention and ability to cause an adverse event, including injury, disruption, damage, theft, diversion, misuse, unauthorized access, intentional release of materials or information, or sabotage.
- **Value or Priority Level:** The relative importance of an asset based on its role in laboratory operations, security and public health impact. High-priority assets typically require stronger security measures due to their critical function or sensitivity.
- **Vulnerability:** A weakness or point of exposure to an attack or other harmful act. In biosecurity, vulnerabilities may exist in electronic security systems, physical features, building design, operational controls, personnel reliability, processes and procedures, information security programs and existing protective forces.

Resources

- APHL Biosecurity Exercises Toolkit for Public Health and Clinical Diagnostic Laboratories, Association of Public Health Laboratories (2024)
- APHL Risk Assessment Best Practices, Association of Public Health Laboratories (2016)
- Biosafety in Microbiological and Biomedical Laboratories (BMBL) Sixth edition, US Centers for Disease Control and Prevention/National Institutes of Health (2020)
- Laboratory Biosecurity Guidance, World Health Organization (2024)
- NIH Guidelines for Research Involving Recombinant or Synthetic Nucleic Acid Molecules, National Institutes of Health (2024)
- Pathogen Safety Data Sheets, Public Health Agency of Canada

Association of Public Health Laboratories

The Association of Public Health Laboratories (APHL) works to strengthen laboratory systems serving the public's health in the US and globally. APHL's member laboratories protect the public's health by monitoring and detecting infectious and foodborne diseases, environmental contaminants, terrorist agents, genetic disorders in newborns and other diverse health threats.

7700 Wisconsin Avenue, Suite 1000 Bethesda, MD 20814 | 240.485.2745 | www.aphl.org

This project was 100% funded with federal funds from a federal program of $790,552. This publication was supported by Cooperative Agreement #NU60OE000104 from the US Centers for Disease Control and Prevention (CDC). Its contents are solely the responsibility of the authors and do not necessarily represent the official views of CDC.