

# Laboratory Biosafety and Biosecurity Risk Assessment Technical Guidance Document

International Biological Threat Reduction, Sandia National Laboratories,  
in collaboration with  
The International Federation of Biosafety Associations



This work was funded by the US Department of State Biosecurity Engagement Program.

<b>Table of Contents</b>	
<b>ABBREVIATIONS.....</b>	<b>5</b>
<b>DEFINITIONS .....</b>	<b>6</b>
<b>SCOPE AND INTENDED AUDIENCE .....</b>	<b>9</b>
<b>I. INTRODUCTION TO LABORATORY RISK ASSESSMENT .....</b>	<b>10</b>
<b>Importance and Benefits .....</b>	<b>10</b>
<b>Risk Communication, Risk Acceptance, and Perceived Risk.....</b>	<b>11</b>
<b>When to Perform and Review a Laboratory Risk Assessment .....</b>	<b>12</b>
<b>Roles and Responsibilities for Risk Assessment .....</b>	<b>13</b>
<b>II. LABORATORY BIOSAFETY AND BIOSECURITY DEFINITIONS.....</b>	<b>16</b>
<b>Complementary Roles of Biosafety and Biosecurity in Biorisk Management.....</b>	<b>16</b>
<b>Laboratory Risks .....</b>	<b>18</b>
<i>Biosafety risks.....</i>	<i>19</i>
<i>Biosecurity risks.....</i>	<i>19</i>
<b>III. LABORATORY RISK ASSESSMENT METHODOLOGY .....</b>	<b>21</b>
1. <i>Define the situation.....</i>	<i>23</i>
2. <i>Define the risks.....</i>	<i>24</i>
3. <i>Characterize the risks.....</i>	<i>25</i>
4. <i>Determine if the risks are acceptable .....</i>	<i>28</i>
5. <i>Implement risk mitigation measures, as needed .....</i>	<i>29</i>
<i>Biosafety Risk Assessment Process Summary .....</i>	<i>30</i>
<b>Biosecurity Risk Assessment .....</b>	<b>31</b>
1. <i>Define the situation.....</i>	<i>32</i>
2. <i>Define the risks.....</i>	<i>33</i>
3. <i>Characterize the risks.....</i>	<i>34</i>
4. <i>Determine if the risks are acceptable .....</i>	<i>38</i>
5. <i>Implement risk mitigation measures, as needed .....</i>	<i>38</i>
<i>Biosecurity Risk Assessment Process Summary .....</i>	<i>40</i>
<b>IV. SCENARIO AND EXERCISES.....</b>	<b>41</b>
<b>Exercise A. Biosafety Risk Assessment .....</b>	<b>42</b>
<b>Exercise B. Biosecurity Risk Assessment.....</b>	<b>47</b>
<b>ADDITIONAL REFERENCES.....</b>	<b>51</b>



## **ABBREVIATIONS**

<b>CWA</b>	CEN Workshop Agreement
<b>IBC</b>	Institutional biosafety committee
<b>IRGC</b>	International Risk Governance Council
<b>ISO</b>	International Organization for Standardization
<b>LAI</b>	Laboratory-acquired infection
<b>GMO</b>	Genetically-modified organisms
<b>OHSAS</b>	Occupation Health and Safety Assessment Series
<b>VBM</b>	Valuable biological materials
<b>VLM</b>	Valuable laboratory materials
<b>WHO</b>	World Health Organization

## DEFINITIONS

### *Adversary*

Individual with malicious intent.

### *Asset*

An item of value.

### *Biohazard*

The potential source of harm caused by biological agents or toxins (Source: CWA 15793).

### *Biorisk*

A combination of the probability of occurrence of harm and the severity of that harm where the source of harm is a biological agent or toxin (Source: CWA 15793).

- The source of harm may be an unintentional exposure, accidental release or loss, theft, misuse, diversion, unauthorized access or intentional unauthorized release.
- Biorisks include both biosafety and biosecurity risks.

### *Biorisk Assessment*

A process of evaluating the biorisk(s) arising from a biohazard(s), taking into account the adequacy of any existing controls, and deciding whether or not the biorisk(s) is acceptable (Source: CWA 15793).

### *Biological facility*

A building or place that includes one or more biological laboratories.

### *Biological laboratory*

A room within a facility, designated for work on biological agents and/or toxins (Source: CWA 15793).

### *Biorisk management*

The analysis of ways and development of strategies to minimize the likelihood of the occurrence of biorisks. The management of biorisk places responsibility on the facility and its manager to demonstrate that appropriate and valid biorisk reduction (minimization) procedures have been established and are implemented. A biorisk management committee should be established to assist the facility director in identifying, developing, and researching biorisk management goals (Laboratory Biosecurity Guidance, 2006).

### *Biorisk management advisor*

An individual who has expertise in the biohazards encountered in the organization and is competent to advise top management and staff on biorisk management issues (Source: CWA 15793).

- Depending on national guidelines and institutional traditions, the role of a biorisk management advisor may be differently named (e.g. biosafety officer, biosecurity officer, biorisk manager, or biorisk management officer).

***Biorisk management system***

Part of an organization's management system used to develop and implement its biorisk policy and manage its biorisks (Source: CWA 15793).

- A management system is a set of interrelated elements used to establish policy and objectives and to achieve those objectives.
- A management system includes organizational structure, planning activities (including, for example, risk assessment and the setting of objectives), responsibilities, practices, procedures, processes, and resources.

***Biorisk mitigation***

Actions and control measures that are put into place to reduce or eliminate the risks associated with biological agents and toxins and other Valuable Laboratory Material (VLM).

***Biosafety risk assessment***

An analytical procedure designed to characterize safety risks in a laboratory. A biosafety risk assessment allows a laboratory to determine the relative level of risks its different activities pose and helps guide risk mitigation decisions so they are targeted to the most important risk. A biosafety risk assessment should consider every activity and procedure in a laboratory that involves infectious disease agents.

***Biosecurity risk assessment***

An analytical procedure designed to characterize security risks in a laboratory. A biosecurity risk assessment should consider every asset as well as every vulnerability in an institution and its component laboratories and units.

***Community***

People outside the workplace potentially affected by the activities of the facility (Source: CWA 15793).

***Harm***

The adverse effect on the health of people, animals, or plants on the environment or on property (Source: CWA 15793).

***Hazard***

A source, situation, or act with a potential for causing harm (Source: CWA 15793).

***Incident***

An event with a potential for causing harm (Source: CWA 15793).

***Insider***

Individual with authorized access.

***Laboratory biosafety***

The set of containment principles, technologies and practices that are implemented to prevent the unintentional exposure to biological agents and toxins, or their accidental release.

***Laboratory biosecurity***

The set of measures aimed at the protection, control and accountability for valuable biological materials (VBM, see definition below) and protection of other valuable items (e.g. equipment) within laboratories, in order to prevent their loss, theft, misuse, diversion of, and/or unauthorized access or intentional unauthorized release.

***Outsider***

Individual without authorized access.

***Risk***

A combination of the probability of occurrence of harm and the severity of that harm (Source: CWA 15793).

***Risk assessment***

A process of evaluating the risk(s) arising from a hazard(s), taking into account the adequacy of any existing controls and deciding whether or not the risk(s) is acceptable (Source: CWA 15793).

***Threat***

The likelihood for an adverse event to occur, as an expression of intention to inflict evil, injury, disruption or damage (Laboratory Biosecurity Guidance, 2006).

***Valuable Biological Material***

Biological materials that require (according to their owners, users, custodians, caretakers or regulators) administrative oversight, control, accountability, and specific protective and monitoring measures in laboratories to protect their economic and historical (archival) value, and/or the population from their potential to cause harm. VBM may include pathogens and toxins, as well as non-pathogenic organisms, vaccine strains, foods, genetically-modified organisms (GMOs), cell components, genetic elements, and extraterrestrial samples (Laboratory Biosecurity Guidance, 2006).

***Valuable Laboratory Material***

Material of value to the laboratory due to its replacement cost and its necessity for the laboratory operational purposes. An example of VLM is laboratory equipment. Such material may be of interest to individuals outside the laboratory for other purposes (e.g. monetary or resource value, illegal drug production, etc.).



## **SCOPE AND INTENDED AUDIENCE**

The scope of this document is to provide technical guidance to all personnel who work in a biological laboratory and who actively handle or manage biological agents and toxins, as well as other valuable laboratory material. This document is also intended for facility managers, administrative support, security forces, community stakeholders, oversight bodies, and policy-makers, who want to learn more about risk assessment and the safety and security risks that are present in their laboratories.

The document describes a generalized risk assessment process - a process that should be used in every biological laboratory setting, regardless of economic or organizational capability. Because risk is a function of likelihood and consequences and a risk assessment is specific to a laboratory's hazards, threats, and work practices, the results of an assessment will undoubtedly vary dramatically between laboratory settings. Further, the risk assessment process does not provide specific recommendations regarding how to reduce the risks identified, but can rather be used to assist or guide individuals in the laboratory, the facility, and the community to make informed decisions how to mitigate risk.

The purpose of this document is threefold: 1) to describe the laboratory biosafety and biosecurity risk assessment process and its conceptual framework; 2) provide detailed guidance and suggested methodologies on how to conduct a risk assessment; and 3) present some practical risk assessment process strategies using realistic laboratory scenarios.

# I. INTRODUCTION TO LABORATORY RISK ASSESSMENT

## Importance and Benefits

*Mycobacterium tuberculosis*, *Brucella abortus*, foot-and-mouth disease virus, *Escherichia coli* O157:H7, *Francisella tularensis*, dengue fever virus - thousands of infectious biological agents and toxins are handled and processed in an assortment of laboratory types for diagnostic, clinical, research, and commercial purposes around the world. The type, number, and quantity of such materials are dependent upon the scope and nature of the work conducted in the laboratory. Each agent and toxin handled is a potential hazard posing a risk to personnel in the laboratory and facility, and likely to surrounding animal and human communities beyond the laboratory.

It is the responsibility of all laboratories that work with valuable biological material (VBM) and other valuable laboratory material (VLM) to operate safely and securely. The first step in achieving this operational goal is to assess the safety and security risks present in the laboratory. This is important during both routine work and unexpected situations. A risk assessment is the fundamental process to aid in the determination, management, and mitigation of laboratory risks. The primary purpose of a laboratory risk assessment is to inform the decision-making process that reduces the risks present in a laboratory. Mitigation of these risks will ultimately protect the individuals in the laboratory, in the facility and/or institution, as well as those outside the biological laboratory, including both the human and animal communities.

The results of a risk assessment provide a guide for the selection of appropriate biological safety measures (including microbiological practices and safety equipment), security measures, and other facility safeguards to mitigate the determined risks to an acceptable or manageable level. In many instances, the results of a risk assessment will demonstrate that some risks can be controlled using relatively straightforward measures, such as properly cleaning up spills and splashes, reducing fall hazards, and locking containers that contain infectious pathogens. Other risks are more problematic and may require greater investment of resources to mitigate them appropriately. It is important to note, however, that while risk assessment is an essential tool to aid in risk reduction, laboratory risk can never be completely eliminated; there will always be risk in a laboratory holding VBM and/or VLM.

The benefits of risk assessment in the laboratory extend beyond risk reduction and mitigation. Laboratory risk assessments can also help to provide the following:

- Effective allocation of resources to mitigate risks
- Identification of training needs and supervision
- Advance planning for renovation
- Evaluation of procedural changes
- Compliance with governmental regulations
- Justification for space and equipment needs
- Evaluation of emergency plans
- Planning for preventative maintenance
- Evaluation of exchanges and workflow with other laboratories/units

The quality of a risk assessment's results is entirely dependent upon the quality of its input data. In other words, a risk assessment requires the collection and input of accurate information. Personnel assigned to contribute to a risk assessment should be thoroughly familiar with the laboratory's work activities, and its biological agent holdings, procedures, equipment, and personnel, as it relates to their contribution to the risk assessment. All information that feeds into the risk assessment process must be collected or assessed by those in the laboratory and who are involved in managing biorisks; this is critically dependent upon drawing from the expertise of laboratory managers, principal investigators, laboratory staff, safety officers, and security personnel, among others.

The international community recognizes the importance of risk assessment to reduce biological laboratory risks. Biological risk assessment may be a legal obligation in many countries and/or be a basis to determine required risk mitigation measures. Many leading guidance documents on biorisk management, including the World Health Organization (WHO) Laboratory Biosafety Manual, the US Biosafety in Microbiological and Biomedical Laboratories, and the international consensus document CEN Workshop Agreement (CWA) 15793:2011 – Laboratory biorisk management (referred to as CWA 15793), emphasize that risk assessment is the fundamental planning step for managing these risks.<sup>1</sup>

Clearly, many laboratories around the world face challenges due to varying levels of organizational and financial resources to mitigate biorisks. Many laboratories do not have the institutional guidance to address their safety or security risks, or the programs and management systems in place are *ad hoc* and not fully supported by management. Other difficulties confronting laboratories around the world include the absence of a reliable electrical supply, inadequate facility infrastructure, geographic and security concerns, volatile weather conditions, and under-trained personnel. Nonetheless, when laboratory personnel decide to utilize a risk-based approach to mitigate the biorisks present in their own laboratories, they become *empowered* to better understand the safety and security risks that affect them, their families, and their communities. They can also take the necessary measures to reduce those risks in a manner that makes the most sense in their constrained environment rather than being held to a prescriptive risk mitigation approach, which may not be attainable or sustainable in such labs. Thus, it is important to recognize that resulting risk reduction measures will vary significantly from laboratory to laboratory, institution to institution, country to country, and region to region.

## **Risk Communication, Risk Acceptance, and Perceived Risk**

The ultimate goal of risk communication is to aid all stakeholders, including laboratory personnel, involved in the risk assessment process to understand the assessment methodologies, results, and risk management decisions. Risk communication is vital to allow laboratory personnel to make informed choices about risks related to their roles in laboratories, and to establish successful biorisk management strategies. Furthermore, strong communication practices will help to establish good reporting mechanisms for any incidents, accidents, or

---

<sup>1</sup>CWA 15793 is based on a management system approach to controlling biorisks and is intended to help laboratories develop a performance-based systematic framework for managing their risks.

mitigation inefficiencies. Risk communication also plays an important role in the laboratory's communication with outside stakeholders, such as regulatory authorities and the general public. Maintaining open communication lines will also be beneficial when conducting future assessments.

Risk assessments should be used as a tool to inform and communicate decisions about the risk by considering the cost and feasibility associated with risk mitigation and benefits derived from the work. Biological laboratories can never eliminate biorisks completely; determining if the risk is acceptable, controllable, or unacceptable is part of the risk assessment process. This determination is referred to as risk acceptance, or risk evaluation.

The acceptability of risk is a subjective value judgment. There are several factors that can influence risk acceptance. These factors include such considerations as the level of available resources to mitigate or control the risks, culture, geographic region, endemicity of the agent or disease in the region, the value of work to the community or to the researcher, the regulatory requirements overseeing the risk, and the public's general perception, among others.

Thus, risk acceptance levels vary according to individual-to-individual or group-to-group. For example, the public perception of risk may vary from that of a technical expert who may be basing risk acceptance on well-characterized risk factors. Yet, public perception of risk can have a strong impact on risk mitigation measures in some cases. A facility must consider the risk perceptions of relevant stakeholders as part of its risk evaluation. The International Risk Governance Council (IRGC) recommends considering the public concerns as a separate analysis from the technical risk assessment (IRGC, 2005). Because risk acceptance is ultimately determined by the user, the emphasis of this document is on the technical assessment and characterization of biorisks.

## **When to Perform and Review a Laboratory Risk Assessment**

A periodic assessment of laboratory risk is important. When experiments, processes, and technology change, so does the risk. A risk assessment should therefore be performed and reviewed periodically - perhaps annually - although an organization should consider conducting a risk assessment more often as circumstances warrant, for example, following the occurrence of problems or if laboratory practices change.

Ideally, a laboratory should perform an initial risk assessment before any work is started. A risk assessment should also be done whenever a change occurs. Examples of activities or events that will change risk and warrant a reassessment include:

- new infectious agents, toxins, reagents or other dangerous substances
- new animal species, model, or route of administration of biological agents
- new procedures and practices
- new equipment
- personnel changes
- aging of equipment
- advances in scientific understanding and technology

- a relocation or renovation
- a recent or “near-miss” accident, laboratory-acquired infection (LAI), theft, or security violation
- national or regional changes in disease status (endemicity of disease or disease eradication)
- national, regional or local changes in threat environment or security environment
- new local or national regulations

After reviewing the results of the risk assessment, measures should be made to amend or update, as necessary. It is important to perform a risk assessment regularly - do not wait until an adverse event happens. Further, each modification or update, as well as each step in the risk assessment process, must be fully documented. Documentation is critical for future reviews when evaluating performance.

## Roles and Responsibilities for Risk Assessment

It is important to emphasize that *a quality risk assessment is the culmination of input from numerous people in the laboratory and/or facility*. The risk assessment process should not be driven or executed solely by a laboratory’s biorisk management advisor.

Further, *risk assessment is an important responsibility* for individuals both within the laboratory and throughout the facility. In an individual laboratory, the best assessors of risk are usually those who work in the laboratory and who are most familiar with the agents and other valuable laboratory materials, as well as the experimental practices and processes. Thus, laboratory biosafety and biosecurity risk assessments should be a shared responsibility between principal investigators, scientists, researchers (or a risk assessment team), and biorisk management advisors. Biorisk management advisors should assume responsibility for initiating the risk assessment process and be vigilant regarding their awareness of all biorisks present within the institution’s laboratories; for a biosecurity risk assessment, campus security forces should also be involved, whenever possible. Descriptions of the various risk assessment users and their responsibilities are provided below:

- ***Biorisk management advisors (alternatively referred to as biosafety officers or professionals)***: These individuals are a member(s) of the staff that provides advice and guidance for laboratory biorisk management issues and workplace risk assessments. These individuals gather relevant information to define risk factors and use that information to characterize risks in terms of likelihood and consequences. The biorisk management advisor should act as a communicator to link hands-on frontline laboratory staff and contractors with managers, higher management staff, and other stakeholders. They should be knowledgeable of laboratory activities, sources of potential exposure, and means of effective control. They should also act as consultants for recommending and implementing appropriate mitigation measures resulting from the risk assessment with support by management. Further, the biorisk management advisors should have the most extensive understanding of a risk assessment’s results.

- ***Principal investigators/scientists/researchers:*** These individuals are the primary providers of information and data input into a risk assessment. They are expected to ensure risk assessments have been completed, understand risk assessment results, and provide input to management regarding practical implementation of recommended mitigation measures. They are also responsible for ensuring that at-risk employees have been informed of the risk assessment results, mitigation measures required, and directing them to obtain specific mitigation measures, whenever needed. The understanding and support of a risk assessment by the scientific staff is critical for effective biorisk management.
- ***External Safety and Security personnel:*** These individuals are experts who may also provide valuable insight into risk assessments. For example, outside agencies such as local police departments may be able to provide information on local threats in the community. Security force personnel may be involved in implementation of biosecurity mitigation measures by management or act as inspectors to check its functionality. Other specialty agencies may also be necessary for the biosafety risk assessments, such as the Hazmat Team, Incident Response, the local fire department, and other first responders. Each group could be called on for additional help in the event of a major safety or security violation that exceeds the response capacity of the institution.
- ***Legal consultant or department/public relations/labor safety officer:*** These individuals have no direct involvement with the risk assessment process. However, expert opinion from this group is valuable when mitigation measures and policy changes need to be circulated among laboratory workers and the general public in order to gain their understanding and support; therefore, their role is instrumental in risk communication. Their opinion may also need to be considered during the risk prioritization process. As these individuals typically are not familiar with a laboratory or laboratory biorisk management, the individual responsible for conducting the risk assessment, such as the biorisk management advisor, should be involved to maximize communication and understanding.
- ***Laboratory contractors, waste handlers, maintenance staff, and janitorial crews:*** These individuals are directly affected by laboratory risks, often with limited knowledge about the hazards to which they are exposed. These individuals should be engaged regarding their concerns and understanding of the risks and how the results of the risk assessment will impact them. This is important to gain their support for implementation of any mitigation measures.
- ***Upper management:*** These individuals, which may include laboratory directors and higher management, will typically not conduct or be directly engaged in the risk assessment process. However, as they are ultimately responsible for the organization's biorisk management system, it is absolutely critical that this group supports (and if necessary, directs) laboratories to conduct risk assessments, including allocating the use of staff time and resources to perform the necessary data collection and analysis.

Upper management will be ultimately responsible for building the infrastructure and capacity that, in turn, supports establishing precautions and standard procedures to minimize laboratory risks. Mutual understanding between the assessor and upper management is essential for maximizing risk assessment outcomes. Resource allocation and financial support from this group is necessary to conduct the risk assessment and implement the appropriate and necessary biosafety and biosecurity measures. Engaging upper management in dialog early in the risk assessment process can reduce confusion when interpreting the results. Early communication can help alleviate miscommunication when management receives the assessment results and must understand the results to make mitigation decisions. It will also be essential that risk assessment results be translated into straightforward terminology to facilitate understanding by upper management.

- ***Administration:*** These individuals have limited access to a laboratory area, but typically have daily access to the people working there. These individuals frequently have no or limited scientific knowledge; thus, communicating technical or scientific assessment results and subsequent policies must be provided in an understandable manner. However, administration should be consulted and engaged in any assessment of risks related to information. Biosecurity measures may heavily affect this population and require their support for facility operation changes.
- ***Community stakeholders:*** These individuals may or may not be engaged, depending on the situation. It may be prudent to inform outside visitors and family of laboratory personnel about any risks they may encounter and how the risks have been effectively managed or controlled.

Once all of the risks have been identified and communicated, the relevant laboratory and institutional staff should work together toward efficiently controlling or reducing the risks to an acceptable level. Stakeholders can work together to determine the necessary biosafety practices (containment) required to perform a task with a specific organism. This should be done in close collaboration with other responsible institutional parties, such as an Institutional Biosafety Committee (IBC) or Biorisk Management Committee, the department of Environmental Health and Safety, and/or any animal care and use committees.

## II. LABORATORY BIOSAFETY AND BIOSECURITY -DEFINITIONS

Multiple definitions of biosafety and biosecurity exist. Moreover, in some languages, biosafety and biosecurity are translated into the same word, and the terms are often not differentiated. The WHO definition of laboratory biosafety is “the containment principles, technologies and practices that are implemented to prevent unintentional exposure to pathogens and toxins, or their accidental release.”<sup>2</sup> More simply, it is a set of practices to reduce the risks of accidental infection. The principles of laboratory biosafety were first introduced by the WHO in 1983 with the first edition of their *Laboratory biosafety manual*; consequently, many laboratories are familiar with the concepts of biosafety and have integrated it to varying degrees into their daily laboratory work in efforts to reduce laboratory-acquired infections.

Laboratory biosecurity is a newer concept and is much less well-known to many laboratories around the world. Further, the term “biosecurity” for those in the animal industry relates to the protection of an animal colony from microbial contamination. For the purposes of this document, laboratory biosecurity, as defined by the WHO, is “the protection, control and accountability for VBM within laboratories, in order to prevent their unauthorized access, loss, theft, misuse, diversion or intentional release.”<sup>3</sup> It is alternatively described as the set of practices to reduce the risks of intentional infection as a result of malicious intent. The advent of laboratory biosecurity was brought about by a number of national and international concerns over developing, implementing, and improving the security of biological agents in laboratories and facilities.

### Complementary Roles of Biosafety and Biosecurity in Biorisk Management

Laboratory biosafety and biosecurity are fundamental biorisk management practices that should be employed in all biological research laboratories. While separate concepts, it is important to recognize that both are complementary and both share a common goal: to keep the laboratory, the community, and the environment safe and secure.

When considering the biosafety and biosecurity measures practiced in a laboratory, one can easily see that the implementation of certain biosafety activities covers some biosecurity aspects, while the application of some biosecurity principles and practices reinforces biosafety. For example, the implementation of locks, badge readers, and/or biometrics are all examples of security measures that can be used to restrict entry of laboratory personnel, as well as any outside individuals or groups, to areas or facilities that house controlled agents – thereby enhancing the security of these materials. Such personnel access restrictions also reduce the overall risk of accidental infection.

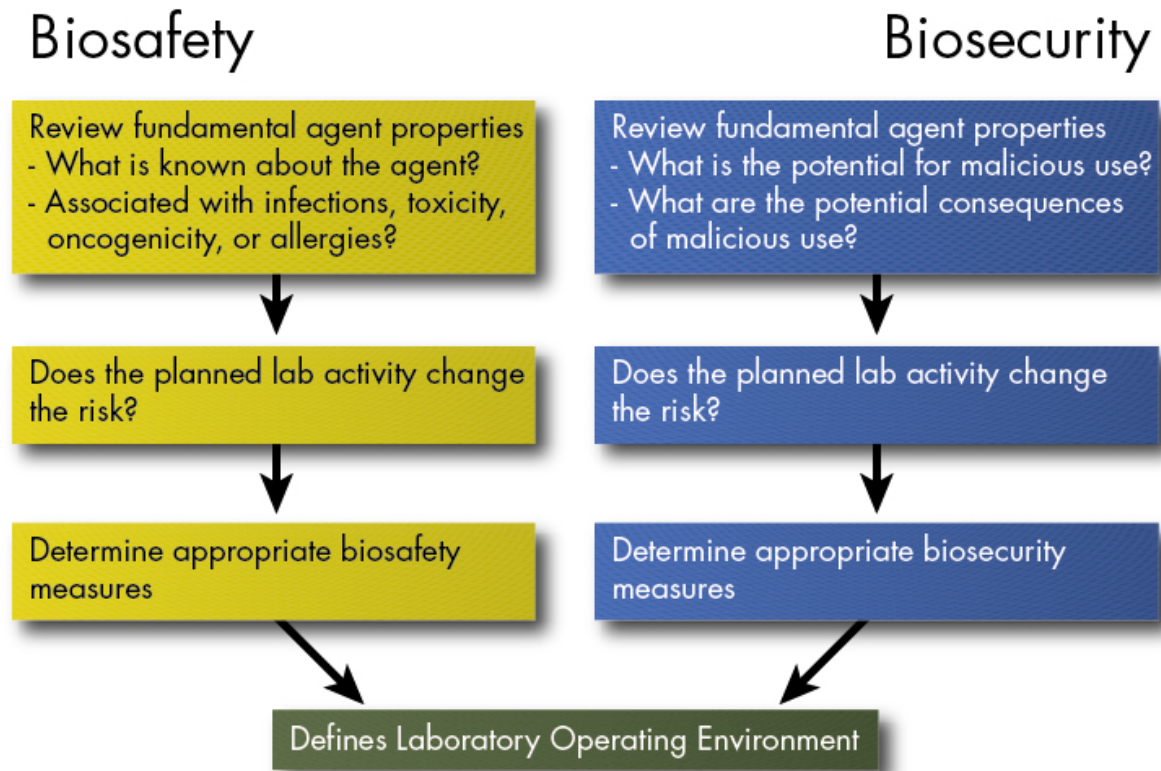
---

<sup>2</sup> WHO (2004). *Laboratory Biosafety Manual*. Available at: [www.who.int/csr/resources/publications/biosafety/Biosafety7.pdf](http://www.who.int/csr/resources/publications/biosafety/Biosafety7.pdf).

<sup>3</sup> WHO (2006) *Biorisk Management: Laboratory Biosecurity Guidance*. Available at: [http://www.who.int/csr/resources/publications/biosafety/WHO\\_CDS\\_EPR\\_2006\\_6/en/](http://www.who.int/csr/resources/publications/biosafety/WHO_CDS_EPR_2006_6/en/)



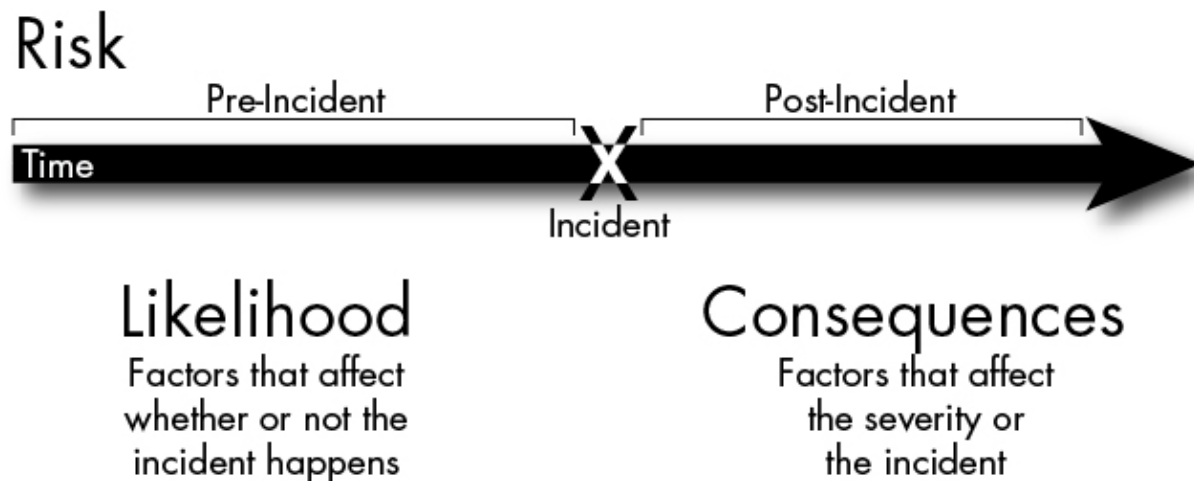
The risk assessment process for both biosafety and biosecurity are very similar; however, separate assessments of their risks are still necessary as the objectives for each process differ (Figure 1). The biosafety risk assessment is concerned with fundamental biological properties of an agent and how the agents are used in the laboratory; for a biosecurity risk assessment, the agent's potential for malicious use are considered, including its consequences of malicious use. Results of both assessments should be similarly reviewed independently, but the implementation of any risk mitigation measures will ultimately be managed in an integrated framework.



**Figure 1. Biosafety and biosecurity risk assessments.** Biosafety assessments (illustrated in yellow) evaluate risks associated with agent and the laboratory processes that are used when handling the agent. A biosecurity risk assessment (illustrated in blue) is focused on an agent's potential for misuse and the consequences of such misuse. Results of both assessments and the implementation of any risk reduction efforts together define a common laboratory operating environment (illustrated in green).

## Laboratory Risks

A broad spectrum of risks may be present in a typical biological laboratory, including risks to individuals working in the laboratory, to the community, and to the environment. To successfully mitigate these risks, it is critical to understand the components of risk. **Risk, in general, is defined as a function of the likelihood an adverse event involving a specific hazard and/or threat will occur, and its consequences.** Risk can also be defined more simply as a function of likelihood and consequences. Likelihood and consequences occur at two different time periods of risk. The likelihood of risk affects whether or not the incident happens, and thus precedes the event. The consequences of risk occur after the incident has happened and affects the severity of the incident. This concept is illustrated in Figure 2.



**Figure 2. Likelihood and consequences of risk.** The likelihood component of risk includes factors that affect whether or not the incident happens and occurs before the actual incident occurs; the consequences component of risk considers factors that affect the severity of an incident after it has occurred.

At the most basic level, understanding a particular risk, therefore, involves answering the following questions:<sup>4</sup>

1. What can go wrong?
2. How likely is it?
3. What are the consequences?

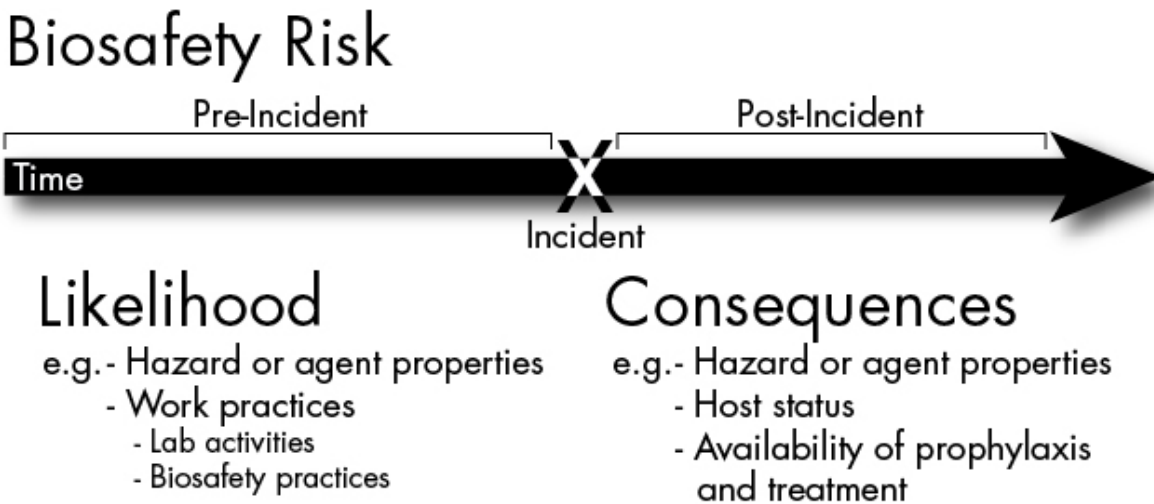
For a laboratory, answering “what can go wrong?” can be a daunting task, but at the simplest level, these include risks posed by the biological agents themselves (e.g. infection via accidental or malicious exposure) and risk to the institution due to theft of intellectual property, valuable property, valuable biological materials, etc. There are also risks inherent to the activities of working with such agents, such as pricking or puncturing the skin with an infected needle or inhaling airborne pathogen particles from poor pipetting technique. All the risks present in a biological laboratory are collectively called “biorisks.”

<sup>4</sup> Kaplan S and Garrick BJ (1981) *On the Quantitative Definition of Risk*. Risk Analysis, Vol. 1, No. 1.

### *Biosafety risks*

Biosafety risks are a type of biorisk that can affect both humans and animals. Personnel working in a laboratory face numerous biosafety risks, especially those that are directly working with infectious agents; biosafety risks exist for personnel working indirectly or in close proximity to infectious agents. Likewise, experimental animals exposed to infectious agents in a laboratory may expose and infect other housed animals in the facility. The public and animal communities outside the laboratory or facility may also face biosafety risks in the event that an agent is unintentionally released into the environment.

While work with any infectious agent or toxin carries a biosafety risk, the severity of the overall risk is dependent upon a number of factors. These factors include 1) properties of the biological agent (also called the hazard), 2) properties of the host, and 3) the work practices and procedures used when handling the agents in the laboratory. A summary of these factors is presented in Figure 3.

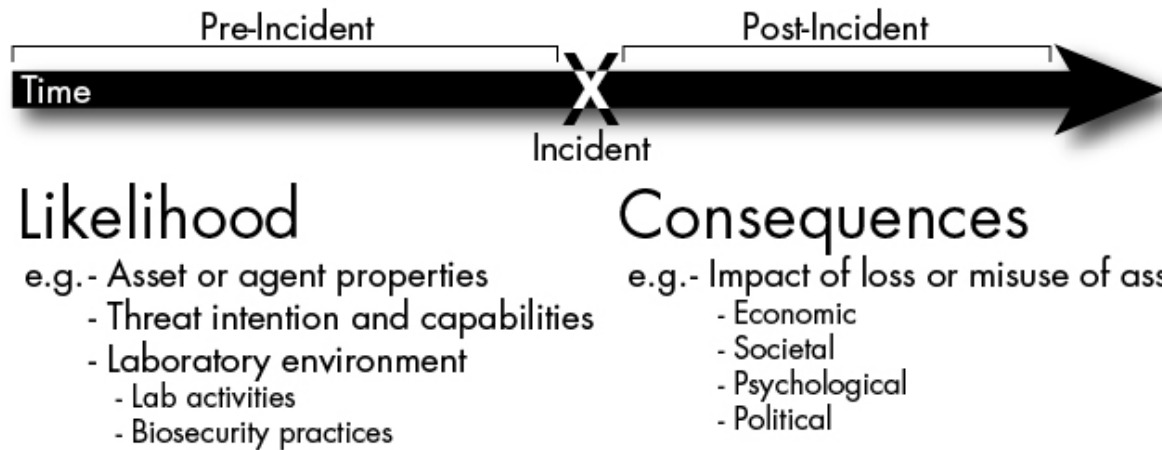


**Figure 3. Biosafety risk**

### *Biosecurity risks*

Biosecurity risks are a type of biorisk based upon malicious intent. These risks are primarily focused on theft of a biological agent(s), equipment, or information, but can also include misuse, diversion, sabotage, unauthorized access, or intentional unauthorized release. The overall biosecurity risk varies with the intent of the adversary (or threat) aiming to do the malicious act. Factors that affect the likelihood and consequences of biosecurity risk are presented in Figure 4.

# Biosecurity Risk



**Figure 4. Biosecurity risk**

In assessing a biosecurity risk, the malicious intent is typically focused upon an item of value, or asset, within the laboratory. In a biosecurity risk assessment, it is critical to define what assets exist within the laboratory. Once the assets are identified, a biosecurity risk can be defined as the likelihood that the asset can be acquired from a laboratory and the consequences of the loss of that asset (to include misuse of the asset following acquisition). Unlike biosafety risks, biosecurity risks are often difficult to identify and characterize because they are dependent upon intent of the individual(s) interested in illicitly attaining and/or using the asset (threat).

Some of the assets which may exist within a biological institution include VBM, VLM (e.g. equipment), intellectual property, informational assets, and intangible assets (such as the institution's reputation). There are many biosecurity risks based upon these assets in biological institutions, and depending upon the situation and the asset, the risks may impact the researcher(s), the facility, the human and animal community, and the economy.

For example, theft of equipment, such as a centrifuge, may present a significant risk to the laboratory researcher who routinely uses the centrifuge for his/her cutting-edge research. Without the centrifuge, the researcher cannot complete his/her work. The impact of this theft could include a financial risk to the researcher if the researcher purchased the centrifuge with his/her research funds. In addition, the loss would present a professional risk to the researcher as his/her work is subsequently halted until a new centrifuge is purchased or borrowed, and during this time, a competing researcher has completed and published the research results first. The biological facility would be impacted by a financial and operational loss. Additionally, the animal and/or human communities may also be at risk if the centrifuge was used maliciously to release an agent into the environment.

### III. LABORATORY RISK ASSESSMENT METHODOLOGY

As stated previously, a laboratory risk assessment should be a structured process to identify and manage the biorisks present within a biological laboratory. A risk assessment reviews all aspects of the work environment, including location, proposed work activities, personnel, storage, sample transfer and transport, destruction, access, and security, among others.

The examples provided within this methodology will be focused on a qualitative risk assessment process. However, *it is important to note that the methodology discussed is also applicable to quantitative or semi-quantitative processes.* Determining when to use the qualitative method or the quantitative method is dependent upon the situation and how one prefers to view and communicate the risk assessment results. It is highly encouraged that the risk assessment team be familiar with both approaches to best fit its needs. There are a number of resources and tools available that can provide more information on how to conduct a qualitative or quantitative risk assessment.<sup>5,6,7</sup>

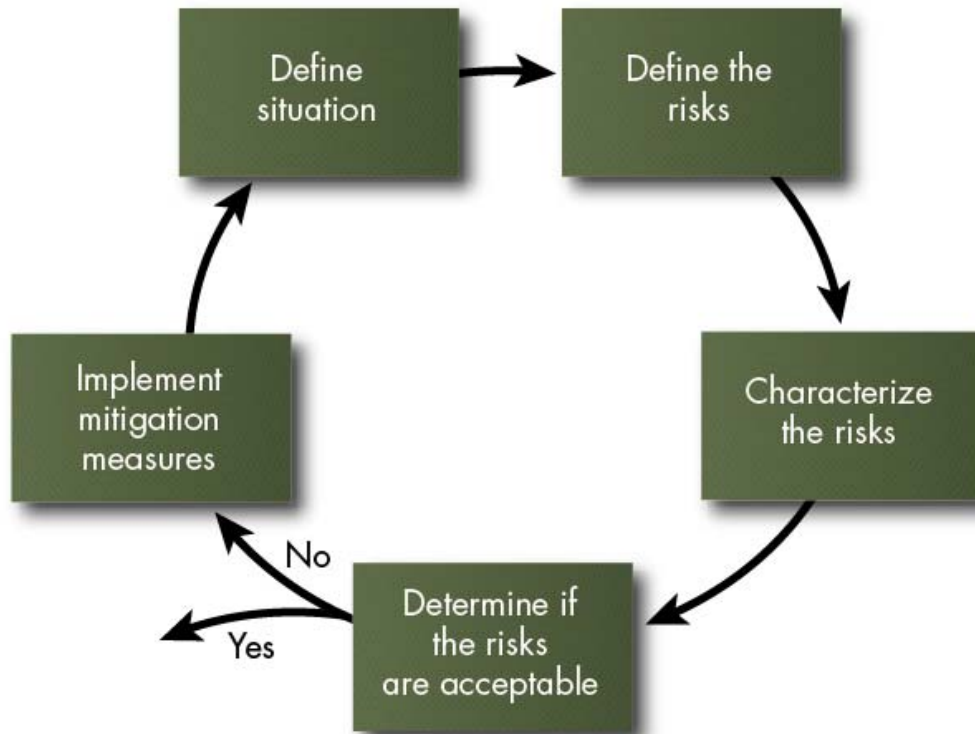
The basic risk assessment process is as follows:

1. Define the situation	<i>What work is occurring?</i>
2. Define the risks	<i>What can go wrong?</i>
3. Characterize the risks	<i>How likely is it to happen? What are the consequences?</i>
4. Determine if the risks are acceptable	<i>Engage management and other key stakeholders</i>
5. Implement risk mitigation measures	<i>Ensure all risks are acceptable post implementation of mitigation measures</i>

<sup>5</sup> Ezell, B, et al. "Probabilistic Risk Analysis and Terrorism Risk" Risk Analysis, Vol 30, No. 4, 2010.

<sup>6</sup> Starr, C. "Hypothetical Fears and Quantitative Risk Assessment. Risk Analysis, Vol 21, No. 5, 2001.

<sup>7</sup> Kaplan, S. and Garrick, B. "On the Quantitative Definition of Risk", Risk Analysis, Vol 1, 1981



**Figure 5. Common Risk Assessment Process**

This section provides guidance on both biosafety and biosecurity risk assessments. As previously stated, separate assessments of safety and security are necessary. Because the objectives of laboratory biosafety and biosecurity are different, the assessed risks will likewise be different.

For a biosafety risk assessment, risk varies with:

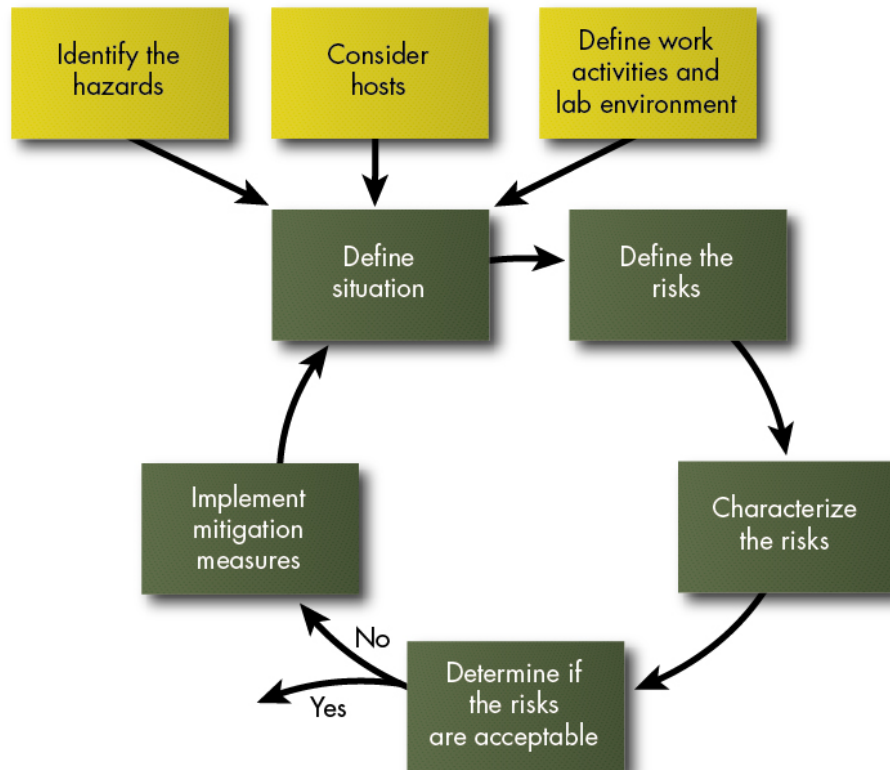
- The properties of the biological agent, the at-risk hosts, and the specific laboratory processes, including any mitigation measures already in place.
- The severity of the consequences to a lab worker or to the environment if there is an exposure and infection.

For a biosecurity risk assessment, risk varies with:

- The likelihood of successful theft of an asset (including VBM) by an adversary (threat) in the institutional environment.
- The severity of the consequences of the theft based upon the properties of the asset stolen and the intent of adversary.

## Biosafety Risk Assessment

A biosafety risk assessment should adhere to a structured and repeatable process and should follow the five-step technical approach described and illustrated below. Factors that affect the likelihood of the biosafety risk are captured in the first step of the risk assessment process, (“Define the situation”).



**Figure 6. Biosafety Risk Assessment Process.** Yellow boxes indicate biosafety specific steps of the risk assessment process; green boxes illustrate common steps shared between biosafety and biosecurity risk assessments.

### 1. Define the situation

#### 1a. Identify the hazards

Hazard identification is a critical step of the biosafety risk assessment process. It helps to answer the question: ***What can go wrong?*** The risk assessment team must identify the biological agents to be used (or possibly suspected to exist if the biological agent in the sample is unknown). Next, it will be important to determine the biological characteristics of each agent to determine how hazardous the agent is (including the potential for the agent to cause disease and the consequences of a disease post-infection). Examples of such information include the agent’s ability to infect and cause disease in a susceptible host, its virulence, the availability of preventative and therapeutic treatments, route of transmission, infective dose, stability in the environment, and host range. This information will be necessary for the third step of the risk assessment process.

## 1b. Consider hosts

The risk assessment team must also consider the host range for the hazards identified. For hazards that can only impact humans within the laboratory, the host range would be limited to the laboratory staff. However, for any agents that have a wider host range, the risks of working with the agent may extend to the agricultural and animal species outside of the laboratory setting in the event of an accidental release (this event would also be dependent upon the endemicity of the agent in the area). For a generalized biosafety risk assessment, a specific review of the potential at-risk hosts may not be needed; however, individuals with compromised immune status who may be exposed to the hazard will require special considerations. This information will be necessary for the third step of the risk assessment process.

## 1c. Define the work activities and laboratory environment

In defining the work activities, the risk assessment team must define and document the laboratory processes, including locations, procedures, and equipment used. The team should also identify those procedures involving biological agents where there is the potential for the generation of aerosols (e.g. pipetting, pumping, centrifugation, sonicating, or vortexing) as well as those utilizing sharps – two common laboratory practices that can lead to laboratory-acquired infections. Further, the concentration and volume of cultures or suspensions of biological agents should be evaluated. This information will be necessary for the third step of the risk assessment process.

## 2. Define the risks

The hazards, hosts, and work activities identified in Steps 1a, 1b, and 1c should be used to define the specific risks to be assessed. This step also helps to answer the question: ***What can go wrong?*** From each activity, there may be one or more agents or procedures which should be considered.

Defining the risks must include a review of the possible exposure routes individuals inside and outside the laboratory may encounter if they come in contact with the hazard(s). These risks include the following examples:

- Risk to individual(s) inside the laboratory
  - Of an infection caused via droplets or droplet nuclei that have entered the upper or lower respiratory tract (inhalational route).
  - Of an infection caused through compromised skin or direct injection into the blood stream (percutaneous route).
  - Of an infection caused through exposure to the mucosal membranes (mucosal route).
  - Of infection caused via contact with the gastrointestinal tract (gastrointestinal route).
  
- Risk to an individual(s) outside the laboratory (the human community)
  - Of an infection caused via droplets or droplet nuclei that have entered the upper or lower respiratory tract (inhalational route).
  - Of an infection caused through compromised skin or direct injection into the blood stream (percutaneous route).



- Of an infection caused through exposure to the mucosal membranes (mucosal route).
- Of infection caused via contact with the gastrointestinal tract (gastrointestinal route).
- Risk to animals outside the laboratory (the animal community)
  - Of an infection caused via droplets or droplet nuclei that have entered the upper or lower respiratory tract (inhalational route).
  - Of an infection caused through compromised skin or direct injection into the blood stream (percutaneous route).
  - Of an infection caused through exposure to the mucosal membranes (mucosal route).
  - Of infection caused via contact with the gastrointestinal tract (gastrointestinal route).
- Risks to humans and animals resulting from a secondary exposure.

After defining the various possible risks present, the risk assessment team should determine if one general assessment will cover all the risks or if multiple assessments are required. It is critical to recognize that the more detailed and specific the assessments are, the more useful the results will be in making risk mitigation decisions.

### 3. Characterize the risks

Risk, as defined previously, is a function of both likelihood and consequences. To determine the risk, one must answer: ***How likely is it to happen?*** and ***What are the consequences?*** To do this, all the elements that influence the likelihood of infection and likelihood of exposure should be considered together to characterize the overall likelihood. One must similarly combine all the elements that define consequences of disease following an exposure to a host to answer what the potential consequences may be. Again, these can be combined mathematically (quantitatively), semi-quantitatively, or qualitatively (as high, medium, or low). Whichever process is used, it is important to document it and be consistent.

#### 3a. Hazard Assessment

In a hazard assessment, one must consider the biological properties of the hazard that would influence its potential (or likelihood) to cause an infection. These would include identification of the routes of infection of the biological agent in the laboratory and the natural environment as well as the agent's infectious dose.<sup>8</sup> The routes of infection within the laboratory should include inhalation, ingestion, injection (into the blood stream), and through mucosal membranes. Additionally, it is important to consider the natural routes of infection, which include vector-borne, sexual transmission, and vertical transmission. These are important in assessing the risk to the human and/or animal community outside of the laboratory and in assessing the potential for a secondary transmission.

---

<sup>8</sup> It is especially important to consider agents with a low infectious dose as they present a greater risk of infection; hazardous agents with a higher infectious dose typically do not warrant similar precautions.

A hazard assessment would also review the properties of the disease(s) caused by the biological agent if an infection occurs or the consequences of the disease. This should include considerations of morbidity (disease) rates, mortality (death) rates, treatment or prophylaxis options, and economic impacts.

### **3b. Host Assessment**

It may not be necessary to assess the potential for an individual person or animal to be infected by the biological agent. However, if individuals have a medical condition or are susceptible to disease due to a weakened immune system, or if the biological agent is unique to the environment (e.g., the biological agent does not currently exist within the environment surrounding the laboratory), consideration of these factors must be documented within the risk assessment process. Further, if a host assessment is deemed necessary, the risk assessment team must consider factors which might influence an individual's potential (or likelihood) of developing an infection, or would influence the potential (or likelihood) of the biological agent establishing a reservoir within the community (environment). It may also be necessary to consider the potential consequences of the disease to specific individuals or to host species within the environment.

In conducting a host assessment, the likelihood of infection and the consequences of disease can be characterized qualitatively (as high, moderate, or low), semi-qualitatively, or mathematically. It is important to document the process used and to be consistent.

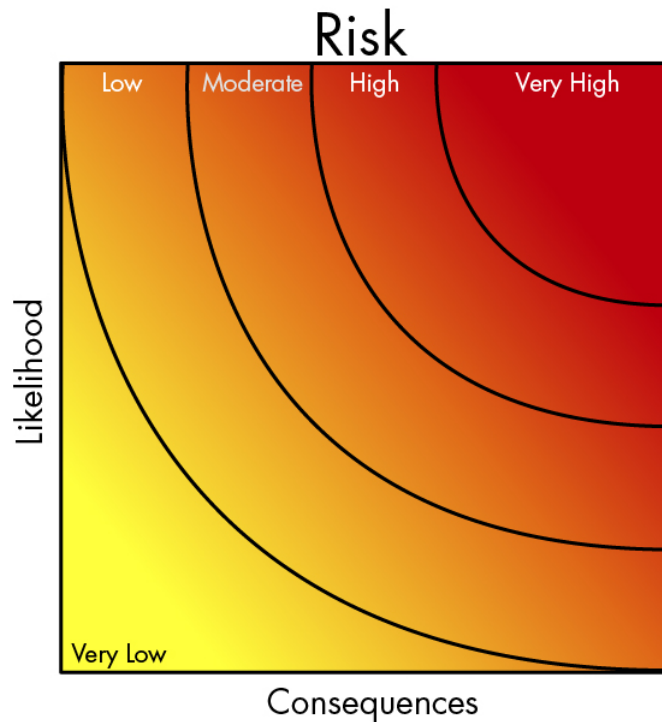
### **3c. Work Activities and Laboratory Environment Assessment**

To assess the risks of the laboratory environment, the risk assessment team should review the types of laboratory processes performed and identify any potential areas where an exposure to the hazard (biological agent) might occur. In addition, it is critical to document and consider any existing biosafety measures that are in place to reduce this exposure. To ensure completeness of the laboratory environment assessment, it is recommended that the team document the potential sources of an exposure separately from existing mitigation measures. This allows for better understanding of how the biosafety mitigation measures directly address the potential (or likelihood) of an exposure to occur.

The team should likewise consider the consequences to the laboratory processes in the event of an exposure that leads to a disease. Such consequences could include loss of program or institutional funding, thus halting research if the laboratory is found to be negligent. Such consequences should be considered and documented.

### **3d. Overall Risk Characterization**

To characterize the overall risk, the overall likelihood would need to be considered as well as the consequence of infection. These can be compared qualitatively, but it is critical that both the likelihood and the consequences be considered when trying to understand risk. These can also be combined using a semi-quantitatively or mathematical process. A two-dimensional graphic provides a good visualization and communication tool when considering the overall risk.



**Figure 7. Typical qualitative two-dimensional graph used to characterize risk.** The area in red in the upper right hand corner represents the highest risk (having the highest likelihood and the highest consequences). The area in the lower left hand corner in yellow illustrates the lowest risk (having both low likelihood and low consequences).

### Risk Characterization Example

The following is an example of the risk characterization process. *It is important to note that this is a simple generalized example of the process and should not be considered a comprehensive risk assessment.*

Let us consider a typical regional diagnostic laboratory. The hazards may include infectious biological agents in the form of diagnostic samples. The potential at-risk hosts include the technicians conducting the diagnostic procedures, and possibly the janitorial and maintenance staff and the community directly outside the laboratory. The work environment, for this case, includes a simple biosafety laboratory with standard laboratory equipment. Based upon this, the biosafety risks (or *What could go wrong?*) include:

1. the risk of a laboratory-acquired infection, due to exposure, to a technician by an infectious biological agent, and
2. the risk of an environmental or community exposure to an infectious agent.

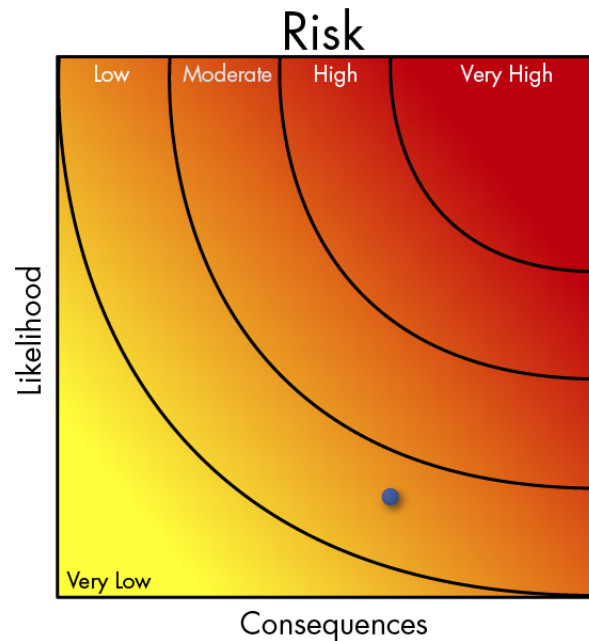
The *likelihood* of, say, a laboratory-acquired infection occurring would be based upon:

- the potential of an infection by one of the possible agents in the sample (if the diagnostic samples are suspected of a food-borne pathogen, the potential for infection would be different than if the samples are suspected of containing an agent which can cause an infection through inhalation) and
- the potential of an exposure based upon the work activities including what types of diagnostic procedures are used and what biosafety measures are in place (for example, in simple serology studies, the potential of an exposure would be less than for someone doing a large volume culture).

The overall likelihood of a laboratory-acquired infection would be fairly low for a food-borne pathogen being analyzed using a small volume kit test as compared to a possible air-borne pathogen (like influenza) existing in the sample which is being cultured in eggs.

The *consequences* of exposure and infection would be based upon the suspected pathogens existing in the samples. Since the samples may contain multiple pathogens, either the worst-case consequences could be considered or a separate analysis for each possible pathogen could be conducted. That is, if the sample is suspected of containing food-borne pathogens, the assessment could consider all potential pathogens that exist within the area and the consequences to a human host of an infection for each of those. Or, the assessment could focus on the worst possible agent that could exist (perhaps a drug-resistant strain of *Shigella*). The consequences of an infection of a drug-resistant strain of *Shigella* could be considered moderate (because of the potential for supportive care while the body responds to the infection, but its drug-resistant properties would have worse consequences than that of the non-drug resistant form of the organism).

To characterize the overall risk, the overall likelihood would need to be considered as well as the overall consequence of infection. Based upon this example, if the sample was suspected of containing a food-borne pathogen and the process for diagnosis was simple (kit-based) and standard good laboratory practices are used, the overall likelihood would be low. The overall consequences would be moderate. As a result, the overall risk of a laboratory-acquired infection would be moderate to low.



**Figure 8. Overall risk graphical summary of the illustrative example described above.** The blue dot represents the result of the risk characterization process showing a low likelihood and moderate consequences.

#### 4. Determine if the risks are acceptable

The risk assessment team, working with management and other stakeholders, should determine if the assessed risk is acceptable to the institution, individuals working in the institution, and the

community. In some situations, the minimal level of acceptable risk may be defined by national or regional policy. For a risk that is determined to be acceptable, the risk assessment results should be documented; for a risk that is determined to be unacceptable, the risk assessment team, management, and other stakeholders must determine which mitigation measures are appropriate to implement and conduct a follow-on assessment once those measures have been implemented.

#### *5. Implement risk mitigation measures, as needed*

The results of the risk assessment will allow an institution to determine the relative level of safety and security risks they face and help guide risk mitigation decisions so they are targeted to the most important risks. Other factors will need to be considered, including finite resources - and the most effective use of these resources to mitigate risk – as well as what type of mitigation measures are the most practical. For example, if a piece of safety equipment is determined to reduce the risk, but it is too expensive for the laboratory or institution's budget and regular maintenance is not possible for the laboratory's location, this risk mitigation measure is not likely to be the best choice.

## Biosafety Risk Assessment Process Summary

A summary of the biosafety risk assessment process and its steps is presented in Table 1.

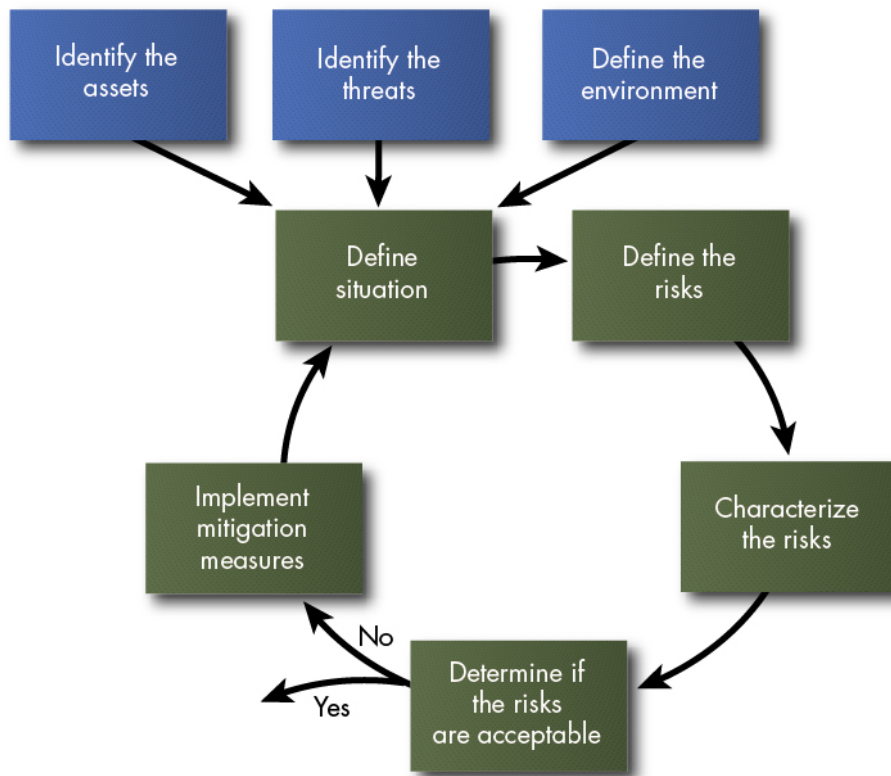
	Step 1	Step 2	Step 3
1. Define the situation	1a. Identify the hazards	1b. Consider the hosts	1c. Define work activities and lab environment
	<p>Create a list of biological agents currently used.</p> <p>What are the biological characteristics of the agents (hazards)?</p>	<ul style="list-style-type: none"> <li>• Lab staff?</li> <li>• Human community?</li> <li>• Animal community?</li> </ul>	<ul style="list-style-type: none"> <li>• Locations?</li> <li>• Procedures?</li> <li>• Equipment?</li> <li>• Manuals and guidelines?</li> </ul>
2. Define the risks	2a. Consider all risks and determine which risks should be defined.		
	Should more than one risk assessment be conducted?		
3. Characterize the risks	3a. Perform a hazard assessment	3b. Perform a host assessment	3c. Perform a work activities/environment assessment
	Define <u>likelihood</u> of infection of the agent.	Define <u>likelihood</u> of infection for staff?	Define <u>likelihood</u> of infection considering the work activities and lab processes used with the hazard.
	Consider <u>consequences</u> to a host of this agent following infection?	Consider <u>consequences</u> of disease from infection.	Consider <u>consequences</u> of an exposure and infection to work practices.
4. Determine if the risks are acceptable	4a. Must be discussed with management and other stakeholders.		
	Must consider lab personnel, institutional personnel and the community		
5. Implement mitigation measures, if needed	5a. Must be discussed with management and other stakeholders.		
	Must consider lab personnel, institutional personnel and the community		

**Table 1. Summary of Biosafety Risk Assessment Methodology Process**

## Biosecurity Risk Assessment

Biosecurity assessments are similar to biosafety assessments, but with a few key differences. A biosecurity assessment includes defining the laboratory assets, threats, and facility vulnerabilities, as well as the existing biosecurity program in place to mitigate biosecurity risks. A biosecurity risk assessment will assess the impact or consequences of potential theft or destruction of the defined assets. Determining the potential security risks based upon these factors is the first step in implementing a biosecurity program.<sup>9</sup>

Similarly to the biosafety risk assessment, a biosecurity risk assessment should follow a structured and repeatable process which clearly defines the likelihood of targeting assets from the laboratory, the likelihood of an adversary (also referred to as the threat) successfully acquiring the target, the institutional environment, and the consequence of a successful acquisition of the asset (and potentially subsequent misuse of the asset) or destruction of the asset. The biosecurity risk assessment process is both described and illustrated below.



**Figure 9. Biosecurity Risk Assessment Process.** Blue boxes indicate biosecurity specific steps of the risk assessment process; green boxes illustrate common steps shared between biosafety and biosecurity risk assessments.

<sup>9</sup> A biosecurity program should be part of a holistic biorisk management program and should be supported by management (or directorship) of a laboratory or facility. A biosecurity program stands upon five pillars—an inventory process, physical security, a personal reliability program, transport programs, and information security processes. A biosecurity program must have an overall program management that supports the five pillars.

## 1. Define the situation

### 1a. Identify the assets

The risk assessment team must identify and document the facility's assets that should be protected. A biological facility will likely have a variety of asset types. Assets include anything of value to the institution or an adversary. Examples of assets may include valuable biological material, such as pathogens and toxins, valuable equipment, intellectual property, or other sensitive information, reagents, and even laboratory animals.

Identification of assets should consider the impact to the facility (financial, reputation, or potential scientific impact) from theft or destruction of the asset and the potential impact to the environment or the facility of misuse of the asset. In considering biological assets, the biochemical properties of biological materials should be considered. This could include difficulty of acquiring, handling, and disseminating the agent, with consideration given to how many other pathways are possible sources for the agent. Specifically characterizing the assets' attractiveness to an adversary and the related consequences will be discussed in detail in Step 3.

### 1b. Identify the threats

Next, the team must identify and evaluate potential adversaries who may pursue those assets. A thorough threat assessment should include a consideration of adversarial types and capabilities, motive, means, and opportunities. It should consider adversary scenarios, as well as consider the likelihood of attack.

Examples of adversarial types that could target assets at a biological facility include competitive researchers, criminals looking for items to sell, disgruntled employees, a terrorist organization, or animal rights activists. These adversarial types can be further categorized into persons with authorized access to the laboratory and/or facility (insiders), and persons with no authorized access (outsiders). There may be graded levels of access to an asset; some insiders may have access to some, none, or all assets. Adversarial motivations to target these assets similarly vary and may include:

- financial gain
- desire to destroy proprietary information
- cause a nuisance by damage or destruction
- inflict casualties
- spread fear
- make a political statement
- protest
- disgruntlement

Whenever possible, the risk assessment team should use the attributes of known adversaries when doing a threat assessment of a facility; this will be critical in characterizing the risk in Step 3. However, this may be difficult if the existing threat environment is not known or very little information is available. It may be necessary to collaborate with security personnel and the local law enforcement team to obtain this type of information. Alternatively, one can create a set of notional adversaries whose attributes span the spectrum of plausible adversaries for the facility. The notional adversaries could be entirely theoretical or could be based on existing data from the



local environment. The local law enforcement community is a good resource to assist in this process, and subsequently, they should be part of the risk assessment team.

### **1c. Define the facility and laboratory security environment**

In defining the environment, the risk assessment team should consider the vulnerabilities of the facility housing the assets. It should also review the work being performed in the laboratory and who has access to the laboratory and its assets. The level of implementation of each pillar will be captured in Step 3.

#### **2. Define the risks**

From the list of defined assets and threats, the risk assessment team can construct a series of potential risks based upon how and why an adversary may attempt to acquire (and possibly misuse or attempt to destroy) an asset.

Risks could include the following examples (the specific risk defined should be unique to the biological institution):

- Risk of an authorized person stealing valuable biological material for malicious use
  - *e.g., an employee upset with spouse and intending to make him/her sick*
- Risk of an unauthorized person stealing valuable biological material for personal gain
  - *e.g., a criminal intending to steal and sell biological material or equipment which contains biological material*
- Risk of an authorized person stealing or destroying valuable biological material for personal gain
  - *e.g., a competitor aiming to publish a strain's information, therefore aiming to acquire a strain or destroy a facility's strain by paying an authorized person to sabotage or steal it*
- Risk of an unauthorized person stealing equipment
  - *e.g., a criminal intending to steal and sell a computer*
- Risk of an authorized person stealing equipment
  - *e.g., an employee stealing a refrigerator for personal use*
- Risk of an unauthorized person stealing an institution's intellectual property (in the form of information) or confidential information
  - *e.g., a competitor aiming to produce a competitive vaccine*
- Risk of an authorized person stealing institution intellectual property (in the form of information) or confidential information
  - *e.g., a disgruntled employee desiring to sabotage institution's reputation by leaking confidential information*

Within each risk there may be one or more assets that should be considered. The location of the assets (both long-term and while in transit) should be documented. Based upon the variety of

locations, and the implemented security and procedures, different assessments may be required for each location. The risk assessment team should determine if one general assessment will cover all locations or if multiple assessments are required. Likewise, the risk assessment team must determine if generalized notional threats can be used in assessing the risk or if specific threats should be considered.

Some situations may not present a sufficient risk to warrant a full assessment. These may include low-risk assets, such as biological materials that are ubiquitous in nature or non-pathogenic to humans or adversaries that are incapable or uninterested in theft. Eliminating unnecessary or unrealistic risks will help narrow the scope to a more manageable size.

### 3. Characterize the risks

Again, biosecurity risk is defined as a function of the likelihood of targeting an asset from the laboratory or institution, the likelihood of successful theft (or acquisition) or destruction of the asset, and the consequences of theft or destruction.

#### 3a. Asset Assessment

Based upon the defined risks, the risk assessment team should define *the likelihood of targeting the asset* by the relevant threat. Depending upon the asset, the defined likelihood will vary. For valuable biological assets, the uniqueness of the asset and any potential for misuse should be considered. For valuable equipment, the value and uniqueness of the equipment and any potential for misuse should be considered. For each of the defined assets, the team should review the various properties that make this asset attractive (or likely) to be stolen or destroyed by an adversary. Similarly, the team should consider what consequences would result in the theft, theft and misuse, or destruction of this asset to the facility, individuals, and/or environment.

The team should likewise consider the consequences of a malicious use or destruction of the asset to both the facility and community (or environment). Additionally, the team should also consider the consequences to the community of an accidental release indirectly caused by the theft or destruction of an asset. This assessment should consider the potential health impact to humans, potential health impact to animal populations, economic impact, psychological and social impact, the financial impact due to the loss of work and/or the cost of replacement, and the possible loss of reputation of the facility resulting from theft and misuse or destruction of the asset.

#### 3b. Adversary Assessment

Define specifically the intentions and access the adversaries might have to each asset to be considered within the assessment; this is key in determination of the vulnerability of the facility to the adversary.

#### 3c. Facility Vulnerability Assessment

Based upon the location of each asset, the risk assessment team should assess *the likelihood of successful acquisition* of the asset based upon the facility's vulnerabilities and the capabilities of the adversary. Consider, in detail, the following facility assessment question (details are included to provide more clarity).

**What are the possible facility vulnerabilities or avenues that an adversary could exploit to gain access to the assets?**

To answer this question, consider the following sub-questions which detail each of the five biosecurity pillars:

- Physical Security
  - For long-term storage areas, what is the physical security situation of the asset?
    - Is it secured? (e.g., is it in a locked freezer?)
    - Is there any means to detect if someone has accessed the agent? (e.g., can one tell if the freezer has been opened?)
  - What is the physical security situation of any rooms where the agent is located (including temporarily)?
    - Is it secured? (e.g., is the room locked?)
    - Is there any means to detect if an unauthorized person enters the room?
  - What is the physical security situation of the building(s) where the agent is located (including temporarily)?
    - Is it secured?
    - Is there any means to detect if an unauthorized person enters the building?
  - What is the physical security situation of the facility or campus?
    - Is it secured?
    - Is there any means to detect if an unauthorized individual enters the facility/campus?
  - If security is breached at any point, what is the response? Onsite response? Local law enforcement?
  - Is the physical security electronic or manual? If electronic, is IT security in place? If manual, is there a key management system in place?
- Personnel Reliability
  - Who has access to the agent?
  - Who needs to have access to the agent?
  - Who has access to the room the agent is in?
  - Who needs to have access to the room?
  - Who has access to the building?
  - Who needs to have access to the building?
  - Who has access to the facility/campus?
  - Who needs to have access to the facility/campus?
- Material Control and Accountability
  - Is information regarding the agent included in an inventory system?
    - When is the agent included in the inventory system? Upon arrival? Upon characterization?
    - Is the inventory updated when the agent is disposed?

- Does this inventory system include the name of a current accountable individual?
- Does this inventory system include detailed information regarding the location of the agent?
  - If so, is the inventory system secure? If on paper, is it physically secure? If electronic, is information technology security in place?
- Information Security
  - What information is considered sensitive?
    - Laboratory research data?
    - Location and types of pathogens?
    - Personnel identifying information?
  - Would an adversary be interested in stealing or sabotaging this information?
  - Is sensitive paper information secure?
    - Is it physically secure?
  - Is sensitive electronic information secure?
    - Is information technology security in place? Are passwords used?
  - Who has access to this data?
- Transport
  - How often are samples transported to and from the lab?
  - Who is involved in the transport process in your laboratory?
    - Are the same individuals responsible for both packaging and receiving?
    - Have they received adequate training in biosafety and biosecurity?
  - How are the biological agents and toxins transported?
    - Car? Bus? Plane?
  - How are the biological agents and toxins stored en route?
    - Is triple packaging used?
  - Who is responsible for transporting the biological agents and toxins?
    - Courier? Designated lab personnel?
    - Have they received appropriate training in the event of a spill or security incident?
  - How are the biological agents and toxins secured between movements?
    - Is chain of custody used?
    - How do these requirements change depending upon the type of biological agent?
  - Do you ensure that the recipient institution has the appropriate level of biorisk management to receive the sample?

Based upon defining the possible facility vulnerabilities or avenues which an adversary could exploit to gain access to the assets in each location they exist, define the likelihood of success of an adversary stealing or destroying an asset. In general, the more positive the responses are to the above sub-questions, the less likely an adversary will be successful.

### 3d. Overall Risk Characterization

To characterize the overall risk, the overall likelihood of targeting (and successful theft or destruction) would need to be considered as well as the consequence of theft or destruction. These can be compared purely qualitatively, but it is key in understanding the risk that both the likelihood and the consequences must be considered. These can also be combined using a semi-quantitatively or mathematical process. Again, a two-dimensional graphic provides a good visualization and communication tool when considering the overall risk.

#### Risk Characterization Example

The following is an example of the risk characterization process. *It is important to note that this is a simple generalized example of the process and should not be considered a comprehensive risk assessment.*

For this example, consider a typical regional diagnostic laboratory; the potential assets may include infectious biological agents in the form of diagnostic samples, test results, and laboratory equipment. The potential adversaries include disgruntled staff (or individuals with access), individuals who are aiming to acquire information regarding test results with malicious intent, and criminals looking for assets to steal and sell. The work environment, for this example, includes a simple biosafety laboratory with standard laboratory equipment and basic security measures. Using this example, the biosecurity risks (or *What could go wrong?*) include:

1. the risk of a theft of an agent by a technician aiming to make others ill
2. the risk of an outsider stealing or destroying laboratory information (specifically test results)
3. the risk of a criminal stealing laboratory equipment, and
4. the risk of an environmental or community exposure of an infectious agent due to theft of laboratory equipment which was contaminated.

The likelihood of, say, the theft of an agent by a technician occurring would be based upon:

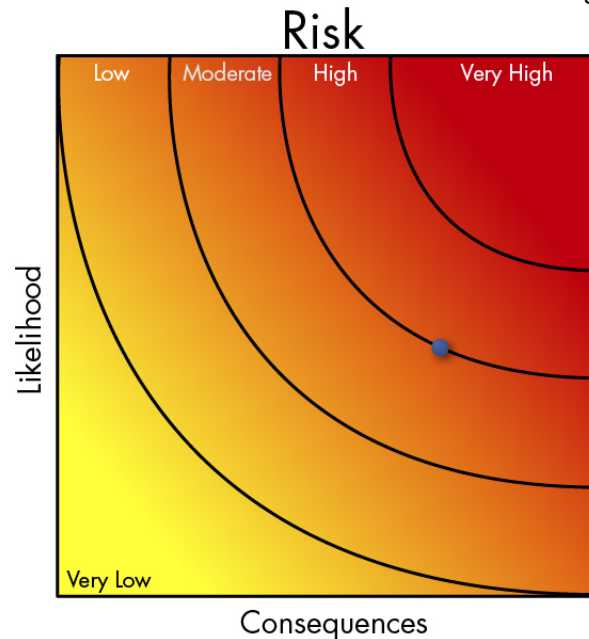
- the aspects of the agent which would make it a target for theft and misuse with the goal to make others ill, and
- the potential of successful theft based upon the facility's vulnerabilities.

The overall likelihood of targeting the agent for theft and misuse, in this example, might be fairly low for, say, a tissue sample from an animal as compared to a cultured sample of a pathogen that is known to make people sick. The likelihood of successful theft and misuse by a technician might be low if the laboratory is fairly small, all the individuals working in the laboratory are well-known to each other, and any potential personal issues are resolved in a positive manner. The likelihood of success might be high if laboratory staff have high turnover and many do not know much about one another. The overall likelihood should be based upon these two factors, and they should be considered together. In this case, there might be a moderate to low likelihood of theft for a laboratory with a high turnover of staff that only has animal tissue samples.

The consequences of misuse of the agent in this example would be based upon the health impact to humans (again, assuming this is the intended goal of the adversaries). This can be determined based upon the disease characteristics. For a culture sample, this would be straightforward since the disease characteristics would be fairly well-known. For the animal tissue sample, the potential of existing zoonotic pathogens existing within the sample that are in a form which could make others ill would need to be considered. For this example, consider the tissue sample. If the sample is brain tissue from a suspected rabid canine, the cerebral fluid has a high potential

of causing rabies in a human host. Without treatment, this disease has a very high morbidity. Thus, the consequences would be high.

To characterize the overall risk, the overall likelihood would need to be considered as well as the consequence of misuse. Based upon this example, the overall likelihood was considered moderate to low. The overall consequences were considered to be high. As a result, the overall risk of a targeted, successful theft and misuse would be moderate to high.



**Figure 10. Overall risk graphical summary of the illustrative example.** The blue dot represents the result of the risk characterization process showing a moderate to low likelihood and high consequences.

#### *4. Determine if the risks are acceptable*

The risk assessment team, working with management and other stakeholders, should determine if the assessed risk is acceptable to the institution, individuals working in the institution, and the community. For some situations, the minimal level of acceptable risk may be defined by national or regional policy. For a risk which is determined to be acceptable, the risk assessment results should be documented. For a risk which is determined to be unacceptable, the risk assessment team, management, and other stakeholders must determine which mitigation measures are appropriate to implement. Once those mitigation measures have been implemented, it would be necessary to conduct a follow-on risk assessment to document how the risk has been reduced.

#### *5. Implement risk mitigation measures, as needed*

The results of the risk assessment will allow an institution to determine the relative level of safety and security risks they face and help guide risk mitigation decisions so they are targeted to the most important risks. Other factors will need to be considered, including finite resources - and the most effective use of these resources to mitigate risk - as well as what type of mitigation measures are the most practical. For example, if a piece of physical security equipment is determined to reduce the biosecurity risk, but it is too expensive for the laboratory or institution's

budget and regular maintenance is not possible for the laboratory's location, this risk mitigation measure is not likely to be the best choice.

## Biosecurity Risk Assessment Process Summary

A summary of the biosecurity risk assessment process and its steps is provided in Table 2 below.

	Step 1	Step 2	Step 3
1. Define the situation	<b>1a. Identify the assets</b> <ul style="list-style-type: none"> <li>• Pathogens?</li> <li>• Toxins?</li> <li>• Equipment?</li> <li>• Intellectual property?</li> <li>• Lab animals?</li> </ul>	<b>1b. Identify the threats</b> <ul style="list-style-type: none"> <li>• What are the adversarial types?</li> <li>• Insiders? Outsiders?</li> <li>• What are their capabilities?</li> <li>• Motives?</li> <li>• Means?</li> <li>• Opportunities?</li> </ul>	<b>1c. Define the facility and lab security environment.</b> Review five biosecurity pillars <ul style="list-style-type: none"> <li>• Physical security</li> <li>• Personnel Security</li> <li>• Material Control and Accountability</li> <li>• Information Security</li> <li>• Transport</li> </ul>
2. Define the risks	<b>2a. Construct a series of potential risks.</b> Construct potential scenarios considering various assets and adversarial types.		
3. Characterize the risks	<b>3a. Asset Assessment</b>  Define <u>likelihood</u> of the asset being targeted.  Consider the <u>consequences</u> of malicious use or destruction of the asset	<b>3b. Adversary Assessment</b>  Define <u>likelihood</u> of an adversary successfully targeting the asset.  Consider <u>consequences</u> of an adversary maliciously using or destroying the asset	<b>3c. Facility Vulnerability Assessment</b>  What is the <u>likelihood</u> of successful acquisition of the asset based upon facility's vulnerabilities  What are the <u>consequences</u> or impact to the laboratory or institution?
4. Determine if the risks are acceptable	<b>4a. Must be discussed with management and other stakeholders.</b>  Must consider lab personnel, institutional personnel, and the community		
5. Implement mitigation measures, if needed	<b>5a. Must be discussed with management and other stakeholders.</b>		

**Table 2: Summary of Biosecurity Risk Assessment Methodology Process**



## IV. SCENARIO AND EXERCISES

### A. Scenario

Researchers are conducting a small vaccine study for a new SARS vaccine. Researchers are growing the SARS virus in multi-liter cell culture volumes (approximately 15 liters of volume). Post-growth and purification, the virus will be inactivated.

The laboratory is a standard BSL2 laboratory space, including: easily cleanable work surfaces, a sink in the laboratory, a Class II B2 biosafety cabinet, and a lockable door. There is an autoclave directly outside the laboratory space. The laboratory does not have directional airflow but the BSC is ducted and HEPA filtered. There is no effluent treatment on the waste water from the sink or emergency shower. Both liquid and solid waste is autoclaved before disposal. The laboratory is locked when not in use and freezers can be locked, but are not typically locked. The laboratory PI and the facility administrative staff have keys, but keys are not provided to other staff. However, facility administration will provide keys to maintenance personnel if requested. The after-hour guard does not have laboratory access.

All equipment is certified/validated on an annual basis. The laboratory also has bench equipment such as incubators and centrifuges as needed for the research. This equipment is also on an annual maintenance cycle.

The facility has a biosafety program which includes introductory training to all new staff on biosafety and biosecurity practices and an introductory training on proper use and storage of PPE, general good laboratory practices which includes inventory management and information protection, and waste handling. There is a formal biosafety manual for the facility, each laboratory is responsible for developing SOPs, however, many laboratories have not drafted laboratory specific SOPs. Personnel working in the laboratory are not formally screened prior to laboratory access, but are interviewed by the PI to determine if they are competent to perform the required activities. The PIs for the laboratory are all long-standing facility employees.

The PPE available for this laboratory includes lab coats (which are autoclaved and washed after each use), laboratory shoes (solid toes and dedicated to the laboratory), goggles, and gloves. There is no formal respiratory protection program for this laboratory and respirators are not used. The laboratory staff includes seven people. One of the staff members is pregnant. Another staff member has been showing irrational and aggressive behavior following a meeting with management that resulted in the loss of an expected promotion.

## Exercise A. Biosafety Risk Assessment

### 1. Define the Situation

#### a. Identify the hazards

- **Hazard:** SARS

**What are the properties of the hazard which would influence its potential to cause an infection in the host? What is the agent's potential to cause disease?**

- Infectious dose is unknown.
- Routes of infection include inhalation, ingestion, contact, and potentially percutaneous route.
- SARS is also communicable person-to-person. No evidence of human-to-animal or animal-to-animal or animal-to-human transmission.

**What are the properties of the disease(s) caused by the biological agent, if an infection occurred in the host? What is the consequence of disease post-infection?**

- Incubation is 2-16 days.
- Mortality (death) rate is 3-15% (WHO estimates that the case fatality ratio of SARS ranges from 0% to 50% depending on the age group affected).
- Morbidity (disease) rate is 3-5 weeks.
- SARS patients generally present with high fever, dry cough, shortness of breath or breathing difficulties, chills, malaise, myalgia, rigors, and possibly, abdominal pain and headache. Symptoms are highly variable.
- No current vaccine is available.
- Economic and social impact would be high if SARS was released into the environment and infected members of the human community.

#### b. Consider the hosts

**Are there any special considerations regarding individuals at-risk (potential hosts) health or immune status which may change the likelihood of them becoming infected by a biological hazard?**

- One staff member is pregnant.

#### c. Define work activities and lab environment

**What are the work practices and in-place mitigation measures which would influence the likelihood that the at-risk individuals could be exposed to the hazard? Consider what work is being conducted and if any current safety mitigation measures are in place.**

- **Locations:** The agent is stored in a -80 freezer in the BSL2 lab. For the experiment, the agent is being grown in 15 liter volumes. These volumes are stored in a laboratory incubator.
- **Procedures:** Cell culture, inoculation, harvesting, purification, formulation, filling, inspection, labeling and packaging.

- **Equipment used:** Pipettes, incubators, centrifuges, filling machines, labeling machines.
- **Mitigation measures:** Staff training, PPE, SOPs.

## 2. Define the risks

### a. Define the possible exposure routes to individuals inside the laboratory if they encounter the hazard.

- Risk to individual(s) inside the laboratory
  - Inhalational route - risk of an infection caused via droplets or droplet nuclei that have entered the upper or lower respiratory tract.
  - Percutaneous route – risk of an infection caused through compromised skin or direction injection into the blood stream.
  - Mucosal route – risk of an infection cause through exposure to the mucosal membranes.
  - Gastrointestinal route – risk of an infection caused via contact with the gastrointestinal tract.
- Risk to an individual(s) outside the laboratory (the human community)
  - Inhalational route - risk of an infection caused via droplets or droplet nuclei that have entered the upper or lower respiratory tract.
  - Percutaneous route – risk of an infection caused through compromised skin or direction injection into the blood stream.
  - Mucosal route – risk of an infection cause through exposure to the mucosal membranes.
  - Gastrointestinal route – risk of an infection caused via contact with the gastrointestinal tract.

## 3. Characterize the risks

### a. Hazard assessment

- **Considering the biological properties of the hazard (described in Step 1a), what is its likelihood of infection of this agent? HIGH? MODERATE? LOW?**
  - HIGH for an exposure via inhalation, ingestion, or contact. Since the infectious dose is unknown it is assumed to have a small infectious dose.
- **Considering the properties of the disease(s) caused by the biological agent, what are the consequences to a host of this agent following infection? HIGH? MODERATE? LOW?**
  - MODERATE to HIGH, as compared to other biological agents that have a much higher death rate and a similar disease rate. The social and economic impact might be high for a short duration of time, but would not have a long-term impact.

### b. Host assessment

**Considering the properties of the hazard's likelihood of infection and likelihood of disease (described above), what is the likelihood of infection for the staff? HIGH? MODERATE? LOW?**

- For six healthy staff – MODERATE
- For the pregnant staff member – HIGH<sup>10</sup>

**c. Work activities and lab environment assessment**

**Considering the work activities and the lab processes used with the hazard, what is the likelihood of infection? HIGH? MODERATE? LOW?**

- **For all staff members** – HIGH, due to inadequate use of PPE (specifically lack of respiratory protection) and/or containment system.
- **For the community** – MODERATE, due to inadequate containment and waste handling, but limited stability of the agent outside of a host.

**Are there any special considerations regarding the consequences to the work practices in the event of an exposure? e.g. loss of funding, community trust, etc. HIGH? MODERATE? LOW?**

- **Loss of funding, societal panic, community mistrust** – HIGH

**Combine the likelihood of the hazard to cause disease, the potential for the at-risk individual to be harmed, and the likelihood of the hazard to cause harm based upon the work activities**

- **Likelihood of the hazard to cause harm?** MODERATE TO HIGH
- **Likelihood of the individual to be harmed?**
  - **Pregnant woman:** HIGH
  - **Other laboratory staff:** MODERATE
- **Likelihood of an exposure to the hazard?** HIGH
- **Overall likelihood of this risk occurring?** MODERATE to HIGH

**Combine the consequence of the hazard causing harm (including any special consequences which should be considered regarding the potential for any at-risk individual), and any consequences associated to the work process itself.**

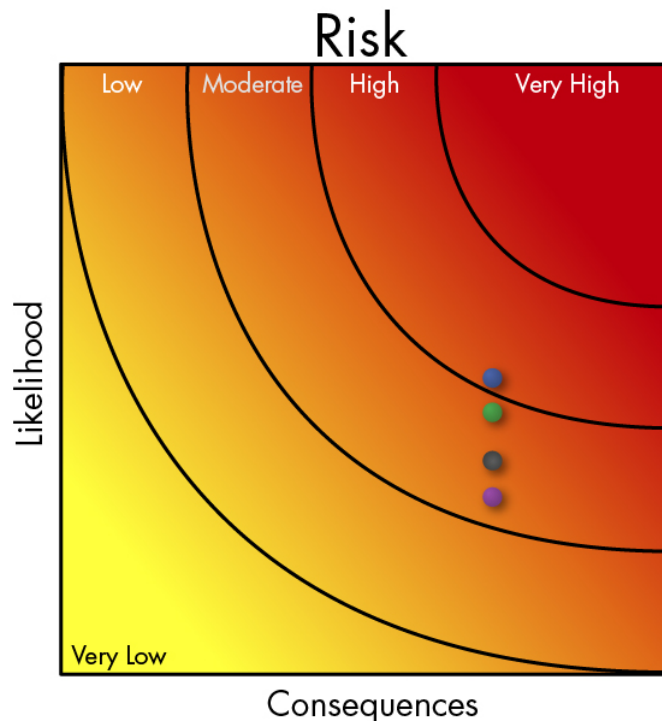
- **Consequence of the hazard causing harm?** MODERATE
- **Specific consequences to at-risk individuals?** MODERATE to HIGH
- **Specific consequences to the work process?** MODERATE

---

<sup>10</sup> Due to the reduced immune response present in pregnant women.

**The overall risks to:**

- Individual(s) inside the laboratory
  - Inhalational route - risk of an infection caused via droplets or droplet nuclei that have entered the upper or lower respiratory tract – HIGH.
  - Percutaneous route – risk of an infection caused through compromised skin or direction injection into the blood stream – MODERATE.
  - Mucosal route – risk of an infection cause through exposure to the mucosal membranes – MODERATE TO HIGH.
  - Gastrointestinal route – risk of an infection caused via contact with the gastrointestinal tract – MODERATE.
- Individual(s) outside the laboratory (the human community)
  - Inhalational route - risk of an infection caused via droplets or droplet nuclei that have entered the upper or lower respiratory tract – MODERATE.
  - Percutaneous route – risk of an infection caused through compromised skin or direction injection into the blood stream – LOW.
  - Mucosal route – risk of an infection cause through exposure to the mucosal membranes - MODERATE.
  - Gastrointestinal route – risk of an infection caused via contact with the gastrointestinal tract – LOW.



**Figure 11.** The above graph maps the risks to individual(s) in the laboratory. The blue dot represents the highest risk, the inhalational route risk. Other risks, percutaneous, mucosal, and gastrointestinal routes, have a lower risk, and are illustrated by black, green, and purple dots.

**4. Determine if the risks are acceptable**

Based upon WHO recommended practices regarding biosafety with SARS and the overall evaluation of risk, these risks would be unacceptable and additional mitigation measures should be required.

#### **5. Implement mitigation measures, if necessary**

Mitigation measures might include relocation of this project to a laboratory with directional airflow and a better waste handling system to reduce the risks to the environment/community and the use of respiratory protection to reduce the risks to the laboratory workers. Other mitigation measures may include respiratory protection, including fit testing, training, and SOP development, training and validation.

## Exercise B. Biosecurity Risk Assessment

### 1. Define the Situation

#### a. Identify the assets

Biological assets:

- SARS agent
- SARS vaccine

Other assets:

- Freezers, incubators, centrifuges, other standard laboratory equipment
- Research data

#### b. Identify the threats

- Insider Adversary – laboratory personnel; specifically, one staff member in particular is disgruntled
- Outsider Adversary – competitive researchers also trying to develop a SARS vaccine, criminals looking to sell lab equipment, any potential terrorist organizations in the area

#### c. Define the facility and laboratory security environment?

**Consider what work is being conducted and if any current security mitigation measures are in place.**

- **Physical Security**
  - Asset security – Freezers can be locked, but not typically locked
  - Room security – The lab is locked when not in use. Only lab PI and facility admin have keys
  - Building security – There is an after-hour guard. Maintenance staff have access.
  - Perimeter security - No information is given
- **Personnel Reliability** – Lab personnel are not formally screened prior to laboratory access, only interviewed by PIs to determine if they are competent to perform job duties, no background checks or formal on-going behavioral assessments, some informal behavioral assessments have been documented.
- **Information Security** - Staff receive introductory training on information protection
- **Material Control and Accountability** – Staff receive introductory inventory management training
- **Transport Security** – No information is given

### 2. Define the risks

**a. Define the possible risks based upon how and why an adversary may attempt to acquire and misuse an asset.**

- Risk of an authorized person stealing valuable biological material for malicious use
  - e.g. an employee upset with management over loss of promotion and intending to contaminate vaccine product
- Risk of an unauthorized person stealing valuable biological material for personal gain
  - e.g. a criminal intending to steal and sell a biological material or equipment which contains biological material
- Risk of an unauthorized person stealing equipment
  - e.g. a criminal intending to steal and sell a computer
- Risk of an authorized person stealing equipment
  - e.g. an employee stealing a freezer for personal use
- Risk of an unauthorized person stealing an institution's intellectual property (in the form of information) or confidential information
  - e.g. a competitor aiming to produce a competitive vaccine
- Risk of an authorized person stealing institution intellectual property (in the form of information) or confidential information
  - e.g. a disgruntled employee desiring to sabotage institution's reputation by leaking confidential information

**3. Characterize the risks**

**a. Asset assessment**

- **Considering the assets, what is its likelihood of targeting the asset by the threat? HIGH? MODERATE? LOW?**
  - HIGH for the disgruntled employee.
  - MODERATE for other laboratory personnel (insiders)
  - LOW for outsiders
- **What would the consequences be of a misuse of the asset?**
  - Malicious release of SARS – HIGH
  - Accidental exposure due to theft of Equipment contaminated with SARS – MODERATE
  - Theft of Equipment – LOW
  - Loss of SARS vaccine details – LOW



## **b. Adversary assessment**

- Insiders – not likely to consider stealing SARS for misuse toward the public, but more likely to steal the research details for personal gain
- Outsiders – not likely to consider stealing SARS for misuse toward the public, but likely to steal equipment and other items of value. May cause accidental release due to theft of equipment.

## **c. Facility Vulnerability Assessment**

**Considering the laboratory and the facility's security environment, what is the likelihood of successful acquisition of these assets? HIGH? MODERATE? LOW?**

- **Physical Security** – HIGH, due to freezers not consistently locked, lab doors only locked after hours, access to all laboratory staff and maintenance crews, if necessary.
- **Personnel Reliability** – HIGH, due to lack of background checks and
- **Material Control and Accountability** – MODERATE, due to minimal training
- **Information Security** – MODERATE, due to minimal training
- **Transport Security** – unknown due to lack of information

**Combine the likelihood of targeting the asset by the threat, likelihood of targeting the asset for misuse or theft by the adversary, and the likelihood of successful acquisition of these assets?**

- **SARS**
  - **Likelihood of targeting the asset by the threat?** MODERATE TO HIGH
  - **Likelihood of the adversary interest or desire to attempt to acquire the asset?** LOW
  - **Likelihood of successful acquisition of these assets?** MODERATE TO HIGH
  - **Overall likelihood of this occurring?** MODERATE to HIGH

**Combine the consequence of misuse of the asset.**

- **SARS**
  - **Consequence of the hazard causing harm?** MODERATE to HIGH
  - **Institution Consequences?** LOW to MODERATE

**The overall risks are:**

- Risk of an authorized person stealing valuable biological material for malicious use - HIGH
- Risk of an unauthorized person stealing valuable biological material for personal gain - LOW
- Risk of an unauthorized person stealing equipment - LOW

- Risk of an authorized person stealing equipment - MODERATE
- Risk of an unauthorized person stealing an institution's intellectual property (in the form of information) or confidential information - LOW
- Risk of an authorized person stealing institution intellectual property (in the form of information) or confidential information - HIGH

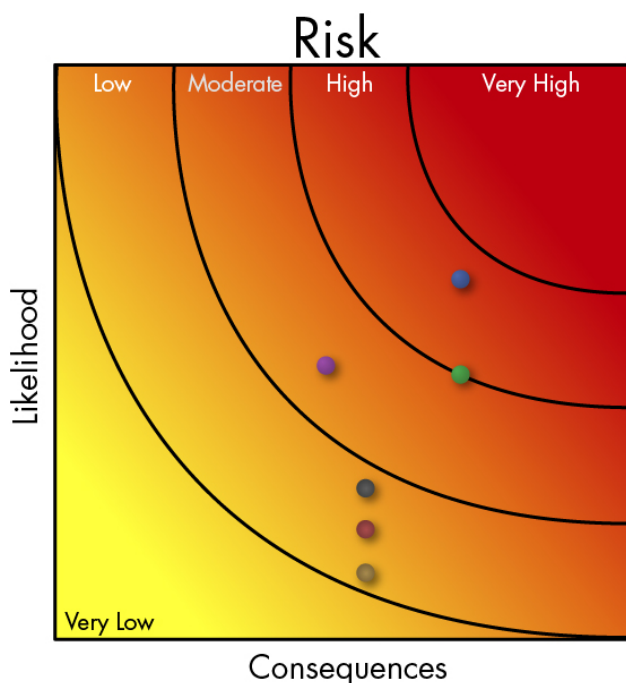


Figure 12. The above graph maps the risks of theft by an authorized or unauthorized person. The blue and green dots represent the highest risk, the risk of an authorized person stealing biological material (blue) or intellectual property (green). The risk of an authorized person stealing equipment is represented in purple. Other risks, such as theft by an unauthorized person, have a lower risk, and are illustrated by black, red, and brown dots.

#### 4. Determine if the risks are acceptable

Based upon recommended practices regarding biosecurity with a dangerous biological agent, these risks would be unacceptable and additional mitigation measures should be required.

#### 5. Implement mitigation measures, if necessary

Mitigation measures might include background checks for all laboratory employees with access to the agent, additional access control types, more intensive training on inventory management and information security.

## **ADDITIONAL REFERENCES**

- A. CWA 15793:2008 'Laboratory Biorisk Management Standard' 2011
- B. CEN Workshop 55 - Guidance Document for CWA 15793:2008 'Laboratory Biorisk Management Standard' 2011
- C. International Risk Governance Council (IRGC). Risk Governance: Towards an Integrative Approach (2005)
- D. World Health Organization (WHO) Laboratory Biosafety Manual (3<sup>rd</sup> edition)
- E. World Health Organization (WHO) Biorisk Management Laboratory Biosecurity Guidance 2006
- F. US Biosafety in Microbiological and Biomedical Laboratories (5<sup>th</sup> edition)