

*Insert Facility/Institute Logo Here*

**BIOSECURITY PROGRAM PLAN *TEMPLATE***

|  |  |
| --- | --- |
|  | |
| Facility: | |
| Manual Title: *Biosecurity Program Plan* | |
| Document Number: *6-01-001* | Version Number: *00* |
| Process Leader: | Effective Date: *MM-DD-YYY* |
| Other documents cross-referenced in this Manual (e.g., manuals, SOPs, forms, records):   * Biorisk Management Manual (*4-00-001*) * Transportation and Shipping Program Plan (*7-01-001*) * *Valuable Biological Material Inventory Management Program Plan (9-01-001)* | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | | | |
| Revision Number | Sections Changed | Description of Change | Date | Approved By |
|  |  |  |  |  |

INSTRUCTIONS: The Biorisk Management Core Document Templates including manuals, program plans, and supporting Standard Operating Procedure (SOP) templates provide a general overview of common considerations and information that should be addressed within a biorisk management system and program. These templates are not exhaustive and facilities must customize each document to ensure it is locally applicable and relevant.

* **Black text** can be considered generic text that may be appropriate for inclusion in a facility’s biorisk management manual and SOPs.
* ***Red text*** should be considered guidance or examples and must be reviewed and replaced with facility-specific information.

Table of Contents

Policies and General Management Page

I. Purpose 3

II. Principle 3

III. Definitions and Terminology 4

IV. Roles and Responsibilities 5

Planning and Assessment Strategies

V. Biosecurity Risk Assessment 8

VI. Emergency and Incident Planning 11

Mitigation Strategies (Five Pillars of Biosecurity)

Pillar 1. Physical Security Systems 14

Pillar 2. Material Control and Accountability 17

Pillar 3. Transportation and Shipping 19

Pillar 4. Information Security 20

Pillar 5. Personnel Reliability 21

Reporting, Monitoring, Response, Review and Revision

VII . Emergency and Incident Response, Reporting and Investigation 24

VIII. Biosecurity Plan Assessment and Improvement 26

IX. References 27

X. Supporting Plans and SOPs 28

Policies and General Management

1. Purpose

The purpose of this program plan is to articulate the specific biosecurity program plan that supports the Biorisk Management Manual that are applicable to and implemented at the *[Insert Facility Name]*. This program plan contains institutional policies, general information about facility operations and references to applicable international and national regulations and guidelines relating to the security of personnel and identified assets of the facility. This plan is supported by a set of standard operating procedures (SOPs) and attachments that describe facility operations and detailed work processes related to the principles described in this plan. This biorisk management core document collection is part of a larger library of manuals, SOPs, and associated job aides that will assist in implementing an overarching facility biorisk management system. These additional documents cover topics such as sample management, diagnostic procedures, and equipment, supplies, facility, information and quality management.

It is the policy of the *[Insert Facility Name]* to provide a safe and secure work environment. By following the guidelines and recommendations herein, the security of the work environment should be improved by minimizing and/or eliminating, where possible, threats to the assets (computers, information and biological) in this facility and ensuring that operations with biological agents and toxins are conducted in a secure and reliable manner. These policies are applicable to all facility directors, managers, investigators, technicians and staff who work at the facility.

1. Principle

The scope of *[Insert Facility Name]* ‘s biosecurity program is to set the requirements necessary to control risks associated with the handling, storage and disposal of biological agents and toxins in the facility. The biosecurity program plan described herein will enable *[Insert Facility Name]* to:

* Establish and maintain a biosecurity plan to control and minimize security risks to acceptable levels as they relate to employees, visitors, the community (animals and people) and the environment, which could be directly or indirectly exposed to biological agents or toxins.
* Provide assurance that the requirements are in place and implemented effectively.
* Provide a framework for training and raising awareness of facility biosecurity guidelines and best practices for personnel.

The management system approach enables *[Insert Facility Name]* to effectively identify, monitor and control the biosafety and biosecurity aspects of its activities. An effective management system approach should be built on the concept of continual improvement through a cycle of planning, implementing, reviewing and improving the processes and actions that an organization undertakes to meet its goals. This is known as the PDCA (Plan-Do-Check-Act) principle which also compliments the AMP (Assessment-Mitigation-Performance) Model approach to biorisk management (**Figure 1**).

|  |  |
| --- | --- |
|  | |
| Figure 1. Illustration of Plan-Do-Check-Act Cycle aligned with AMP Model for biorisk management [adapted from ISO 35001 : 2019, Biorisk management for laboratories and other related organisations] | |
| Plan | Planning, identification of hazard and risk and establishing goals |
| Do | Implementing training and operational issues |
| Check | Checking, monitoring and corrective action |
| Act | Reviewing, process innovation and acting to make needed changes to the management system |

This manual serves to demonstrate that the *[Insert Facility Name]* recognizes the documents listed below as informative references and seeks compliance through risk-based, sustainable approaches:

* + - WHO Laboratory Biosafety Manual, 4th Edition
    - WHO Biorisk Management: Laboratory biosecurity guidance, September, 2006
    - ISO 35001 : 2019, Biorisk management for laboratories and other related organisations

1. Definitions and Terminology [Adapted from ISO 35001: 2019, Biorisk management for baboratories and other related organisations and WHO Laboratory Biosafety Manual, 4th Edition definitions]
2. Accident-An occurrence arising out of, or in the course of, work that does result in harm.
3. Biohazard-Potential source of adverse effect, caused by biological materials, on the health of people, animals, or plants, on the environment or on property
4. Biological agent-Any microbiological entity, cellular or non-cellular, naturally occurring or engineered, capable of replication or of transferring genetic material that may be able to provoke infection, allergy, toxicity or other adverse effects in humans, animals, or plants
5. Biorisk-Effect of uncertainty expressed by the combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence, where biological material is the source of harm
6. Biorisk management system-Set of interrelated or interacting elements of an organization to establish policies , objectives , and processes to achieve those objectives to establish the control of biorisk(s)
7. Biosafety-Practices and controls that reduce the risk of unintentional exposure or release of biological materials
8. Biosecurity-Practices and controls that reduce the risk of loss, theft, misuse, diversion of, or intentional unauthorized release of biological materials
9. Decontamination -Procedure that eliminates or reduces biological agents and toxins to a safe level with respect to the transmission of infection or other adverse effects
10. Disinfection- A process to eliminate viable biological agents from items or surfaces for further safe handling or use
11. Incident- Occurrence arising out of, or in the course of, work that could result in harm
12. Sterilization – A process that kills and/or removes all biological agents including spores
13. Toxin-Substance, produced by plants, animals, protists, fungi, bacteria, or viruses, which in small or moderate amounts produces an adverse effect in humans, animals, or plants
14. *Others to be determined*

1. Roles and Responsibilities [Adapted from ISO 35001: 2019, Biorisk management for laboratories and other related organisations and WHO Laboratory Biosafety Manual, 4th Edition descriptions]

The responsibility for assuring safe and secure handling of biohazardous materials is shared between the employee, their supervisor (scientific management), top/senior management (administrative or financial managers), security personnel, and the *[Insert Facility Name]* Biorisk Management personnel. These responsibilities are described generally below. More specific duties are outlined within the relevant SOPs.



*[Insert your facility’s organizational chart here]*

1. **Top and Senior Management** *Top management shall take ultimate responsibility for the organization’s biorisk management system. Top management shall not delegate its ultimate responsibility, but may delegate authority. Top management shall demonstrate its commitment by ensuring the availability of resources to establish, implement, maintain, and improve the biorisk management system. Senior management shall be designated with operational responsibility for overseeing the biorisk management system and ensuring the implementation of the operational function of the biorisk management system.*

*These functions include:*

* + - *ensuring the provision of appropriate and adequate workers, facilities, and other resources deemed necessary for the safe and secure operation of the facility;*
    - *reporting to top management on the performance of the biorisk management system and any need for improvement;*
    - *ensuring promotion of the biorisk management system throughout the organization; and*
    - *instituting review, audit, and reporting measures to provide assurance that the requirements of this document are being implemented and maintained effectively.*

1. **Biorisk Management Committee** *A biorisk management committee shall be established in support of the biorisk management system. Where feasible based on the nature of the organization and its activities, the committee shall consist of members who are independent of activities being reviewed for biorisk issues.*

*The committee shall establish a mechanism by which committee members shall recuse themselves from participation in committee decision-making procedures (e.g. a vote) on issues where real or perceived conflicts of interest exist.*

*Reporting to senior and/or top management, the committee shall:*

* + *have documented terms of reference;*
  + *include a representative cross-section of expertise, appropriate to the nature and scale of the activities undertaken;*
  + *ensure issues addressed are formally recorded, including the assignment, tracking, and completion of all actions;*
  + *be chaired by someone appointed by senior and/or top management; and*
  + *meet at a defined and appropriate frequency, and when otherwise required.*

*NOTE The responsibilities of the committee can be assumed by other existing committee(s), such as an Institutional Biosafety Committee (IBC) or other biosafety committee.*

1. **Biorisk Management Advisor** (or Biosafety Officer) Competent individual(s) designated to provide advice, guidance, and assurance on biorisk management issues. This individual shall report directly to the responsible senior management and have delegated authority to prohibit work in the event that it is considered necessary to do so. This role shall be independent of those responsible for implementing the program of work.

Functions of the biorisk management advisor should include:

* + - * verifying, in conjunction with other workers, that all biorisks have been addressed;
      * advising or participating in the reporting, investigation, and follow-up of accidents, incidents, and, where appropriate, referring these to management/biorisk management committee;
      * ensuring that relevant and up-to-date information and advice on biorisk management is made available to scientific and other workers as necessary;
      * advising on biorisk management issues within the organization (e.g. management, biorisk management committee, occupational health department, security);
      * contributing to the development and/or delivery of biorisk management training activities; and
      * advising and assisting organization management in ensuring that required authorizations for work are in place.

NOTE Examples of biorisk management advisor roles include biosafety professionals, biological safety officers, biosafety practitioners, biosafety coordinators, biosafety responsible officials, biosafety advisors, or

equivalent.

1. **Scientific Management** *Individual(s) with responsibility for all or part of the science program at the facility shall also be designated with specific biorisk management responsibilities.*

*Functions shall include:*

* + - * *planning and coordinating work activities, and ensuring adequate staffing levels, time, space, and equipment are available;*
      * *ensuring (where necessary in consultation with the biorisk management advisor), that hazard identification and risk assessments have been performed, reviewed by all affected workers, subjected to approvals required by the biorisk management system, and that the required control measures are in place;*
      * *ensuring required authorizations for work are in place;*
      * *ensuring that all at-risk workers have been informed of risk assessments and control measures, and/or provisions for any recommended precautionary medical practices;*
      * *ensuring that all work is conducted in accordance with established policies and guidelines described in this document;*
      * *supervising workers, including ensuring only competent and authorized workers have access and can work in areas under supervision; and*
      * *ensuring that processes are in place to routinely measure the effectiveness of the control measures, and to change the control measures as appropriate to improve biorisk management performance.*

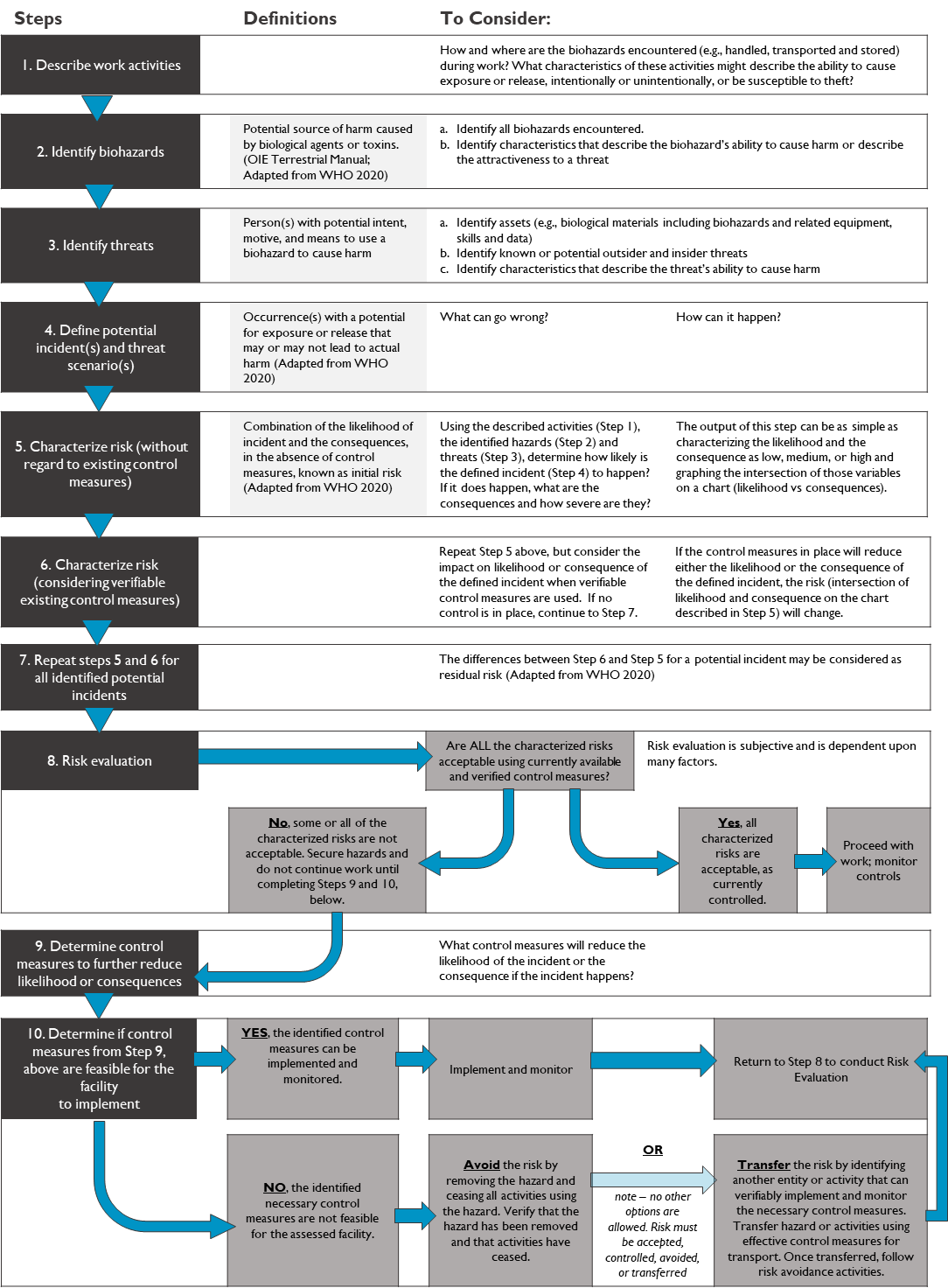
1. **Occupational Health** *The employing authority, through the facility director, must take responsibility for ensuring that the health of facility personnel is adequately checked and reported*
2. **Facilities Manager**(s) *Are responsible for equipment and facilities, typically an engineer with an in-depth knowledge of the facilities, containment equipment and buildings, coordinating building and maintenance work, and liaising with contractors.*
3. **Security Manager** *shall be designated with responsibilities to implement effective and proportionate facility biosecurity measures, based on the biological risk. This position requires an in-depth knowledge of facility security.*
4. **Animal Care Manager** *shall be designated with responsibilities determined in accordance with country-specific requirements for proper animal care and use in work areas where animals are maintained. This position requires an-depth knowledge of animal handling and zoonotic and animal diseases with a qualified veterinarian available for additional advice.*

Planning and Assessment Strategies

Proper planning of work activities is the first critical step in establishing and maintaining abiosecurity program plan. Threats and assets must be identified, characterized, and assessed to facilitate proper selection of control measures and determination of risk acceptance. Specific elements of planning and assessment strategies to ensure proper response and continuity of operations include: threat identification and assessment, identification of the assets to be protected, vulnerability assessment, legal requirements, personnel needs, and emergency plans.

1. Biosecurity Risk Assessment

A biorisk assessment methodology is shown in Figure 2 on the following page. This is useful when considering biosafety and biosecurity assessments.

** Figure 2** : Risk Assessment Diagram

Facility-specific biosecurity risk assessments follow the same principles outlined in the Biorisk Management Manual for biosafety, but also are required to ensure adequate security measures are in place to reduce the risk of the theft and misuse of biological agents. The objective of a biosecurity risk assessment is to develop a strategy to manage biosecurity risk, including a threat assessment to determine the likelihood of theft of a biological agent, and the severity of the consequences associated with an attack by that agent. Based on the risk identified, the vulnerabilities in a facility’s current biosecurity program can be identified and adapted to ensure unacceptable biosecurity risks are reduced to levels deemed acceptable by facility stakeholders. The risk assessment should also include a clear definition of the threats the system is designed to protect against. These threats should be articulated in a Design Basis Threat (DBT) statement that details the threat and clarifies the mission and performance requirements of the biosecurity system. Relevant factors to consider when conducting a facility biosecurity risk assessment are listed in Table 2 however, not all of these factors will impact risk in the same manner.

|  |  |
| --- | --- |
| Table 1. Facility-Level Biosecurity Risk Assessment Factors | |
| **Characterize Assets** | Identify Malicious Use Properties of the Assets (Valuable Biological Materials) |
| **Develop Design Basis Threat** | Determine Which Assets Will be Assessed  Determine Which Adversaries Will be Assessed   * Characterize Threats (e.g., adversary type, capabilities and methods, motivation)   Determine Which Scenarios Will be Assessed   * Specify characteristics of event |
| **Evaluate Scenarios** | Assess Likelihood and Consequences of Malicious Use  Assess Adversaries (Threat Assessment)  Assess System Performance |
| Identify and Assess Vulnerabilities |
| **Characterize the Risk** | Risk Evaluation   * Not Tolerable * Tolerable * Acceptable |
| Available Risk Reduction Strategies   * Mitigation Measures (Facility and Equipment Upgrades, Adapted Practices) * Analysis of Alternatives |
| * Cost-Benefit Analysis |

In summary, when conducting biorisk assessments it is important to acknowledge that while biosafety focuses on keeping the workers, human, and animal community safe, and biosecurity focuses on keeping the valuable assets inside the facility secure, these two goals might not always be synergistic. It is important to have both aspects in mind when deciding upon a relevant biorisk management strategy and actual mitigation measures.

*[Insert Facility Name] uses a variety of tools for risk assessments, including Facility Biosafety and Biosecurity (BS&S) Assessment Forms and a Protocol Risk Assessment Form (refer Biological Risk Assessment Forms and Checklists). These forms are completed by Scientific Managers for review and approval by the Biorisk Management Advisor and Biorisk Management Committee. [Provide additional details about review and approval process below, or write supporting SOP to be referenced]*

* *Who is responsible for completing risk assessments?*
* *How are risk assessments reviewed (e.g., low risk by Biorisk Management Advisor, high risk by committee)?*
* *How does the facility ensure reviews are conducted by individuals with appropriate expertise?*
* *How is risk acceptance determined?*
* *Does the facility have a DBT that includes: identification of assets (e.g., biological, information, equipment, facility), identification of the insider (e.g., employees, visitors) and outsider adversaries (criminals, terrorists, extremists/activists), attributes and characteristics of adversaries (to include capabilities, weapons, and tactics likely to be employed), and potential types of malicious attacks (scenarios). How is the information in the DBT protected and controlled?*

1. Facility Emergency and Incident Planning

Even the most well-prepared facility may experience accidental or intentional incidents or emergencies such as fire, biological release, chemical spill, or minor workplace injuries despite existing prevention or mitigation measures. Effective incident response is a mitigation strategy that may reduce the consequences from these unknown events through planning, and preparing for potential incidents, as well as detecting, communicating, assessing, responding to and recovering from actual events. Design Basis Threat assessment scenarios can be used for response planning activities. Facilities should have a documented contingency plan for incident and emergency identification and response. Plans should be developed at a senior management level and incorporate feedback from frontline staff.

Planning considers the potential incidents and designates resources to respond to threats and mitigate outcomes. These potential incidents should consider the risk assessment for an individual work area and the facility as a whole. Common potential incidents to be included in a facility emergency and incident plan should include, but are not limited to:

* Puncture wounds, cuts, and abrasions
* Personnel exposure to potentially infectious materials
* Broken containers and spilled infectious substances
* Biohazard spill outside primary containment (biosafety cabinet, centrifuge)
* Fire and natural disasters (tsunami, hurricane, earthquake, power outages)
* Security breaches or incidents involving malevolent human adversaries (crime, arson, terrorism, vandalism, civil disobedience)
* Missing valuable biological materials from inventory

Acquisition of resources, storage, and equipment, and provision of personnel training and facility drills is essential in preparing for and managing an incident or emergency. *[Provide additional details about your Emergency and Incident Planning process below, or write supporting SOP to be referenced]*

* + *Determine the signal for emergency or incident response operations*
  + *Identify high-risk agents and assets*
  + *Identify high-risk areas (work areas, storage areas, etc.)*
  + *Identify at-risk personnel and populations*
  + *Identify responsible personnel and their associated roles and responsibilities during an emergency or incident response. Identify an Incident Commander to ensure a smooth transition from normal operations to emergency operations. Members of an incident response team can include: Security personnel, Biorisk Management Advisor, Safety personnel, Scientific Director, Facilities personnel, Occupational Health, local first responders, and other individuals as needed. [List your Incident Commander and response team by titles here]*
  + *Identify agreements necessary to coordinate with local emergency, fire, law enforcement and first response entities*
  + *Identify local or national regulations that might impact response to an incident or emergency*
  + *Management needs to provide, and staff need to be able to locate emergency first aid kits and other tools such as spill kits, personal protective equipment*
  + *Determine the signal to return to normal operations*

Drills and exercises can also be used in the planning and preparation stages to test the responses to simulated incidents or emergencies. They can help identify gaps and other improvement opportunities. Plans should be reviewed and updated at least annually incorporating the information garnered through drills and incident reports and investigations. Plans should take into consideration the steps between event occurrence and identification and reporting. A standard reporting chain should exist to facilitate reporting. Incident report forms are available to provide an opportunity for investigation, root cause analysis, corrective action, and process improvement (refer to Biorisk Management Manual Core Document, Chapter XXI. Emergency and Incident Response, Reporting and Investigation).

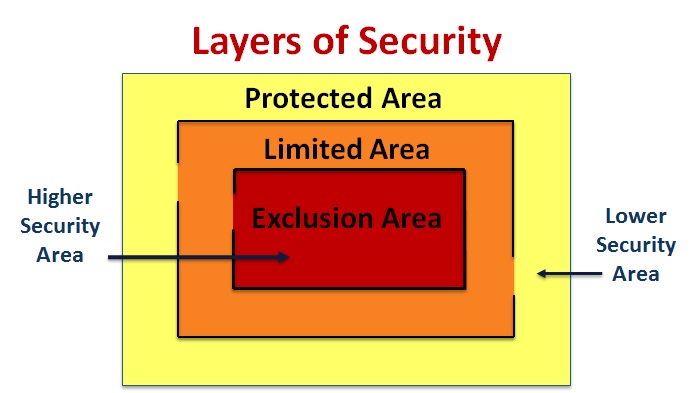
Mitigation Strategies

Once planning and assessment strategies are effectively implemented, a variety of mitigation strategies can be implemented to reduce biosecurity risk to an acceptable level. The following sections detail the five pillars of biosecurity that categorize the primary focus of mitigation controls. These controls work together to prevent or minimize accidental or intentional release of potentially infectious materials that may occur during the course of normal operations at *[Insert Facility Name].*

The five pillars of biosecurity mitigation strategies should be guided by the two basic concepts of graded security and balanced security.

Graded protection is the concept of increasing security measures as you move from outside low security areas (public access areas) into the more internal high security areas (exclusive access areas) in a graded fashion based on a risk assessment. The idea is to have layers of security where the most valuable assets are afforded the highest levels of security (See Figure 3).

Balanced security is the concept of creating equal mitigation layers for an adversary to face, regardless of path chosen to the targeted asset. In Figure 3, this would mean having the same level of protection moving from the protected area into the limited area from either entrance (right or left doorway). This would also mean having equal quality of materials for the perimeter of each layer of security. Having easily-broken windows, or weak door materials with a sophisticated door lock is unbalanced.



**Figure 3.** Layers of Security to evaluate graded protection and balanced security.

**The Five Pillars of Biosecurity Mitigation:**

1. Physical Security

Physical security countermeasures are used to prevent unauthorized access from outside adversaries (i.e., those who do not have a legitimate presence in the facility and harbor malicious intent such as criminals, terrorists and extremists/activists) and also minimize the threat from insiders (i.e., those who have a legitimate presence in the facility such as employees and approved visitors) who do not require access to a particular location and asset. Physical security systems promote not only biosecurity objectives, but directly support biosafety by limiting access to the work areas and other potentially hazardous spaces to those individuals with the appropriate training. An effective physical security system incorporates a variety of elements to enhance a facility’s capability to detect, assess, delay, respond to, and recover from a security incident. These elements include establishing boundaries, access controls, intrusion detection and alarm assessment, as described in more detail below, and are typically used in a graded manner. A graded protection system is achieved by increasing security incrementally and forming concentric layers of protection around the facility’s assets in a risk-based manner. The highest level of protection should be given to those primary assets whose loss, theft, compromise, and/or unauthorized use will most adversely affect international or national security, and/or the health and safety of employees, the public, and the environment. In addition, these elements are selected and implemented following a facility- or site-specific biosecurity risk assessment to ensure that all elements are practical, sustainable and commensurate with identified risks (refer to Chapter V, Biorisk Assessment).

* 1. Perimeters and Boundaries

Boundaries are established to demarcate areas that are under some level of access limitation. Signage, landscaping, and in some cases fencing, which is also a type of access control for personnel and vehicles, can be used for property demarcation. Other boundaries for restricted areas include walls, windows and doors. Considerations must be made for daily foot traffic and emergency egress. *[Describe how perimeters and boundaries are demarcated]*

* *Is there graded protection?*
* *How are access limitations marked or visualized (i.e., signage, fence, landscaping)*
* *How are walls, windows, doors secured?*
  1. Access Controls

The goal of an access control system is to allow authorized persons to enter secure areas and prevent or delay the entry of unauthorized persons into secured areas. Access controls provide reasonable assurance that only authorized personnel are allowed to enter a restricted area. The type and number of controls depend on the level of security required. Access can be controlled with a variety of unique items (e.g., badges, physical or electronic keys, knowledge (PIN code), biometrics). These items can be used in combination or sequentially to increase the probability that and individual is indeed authorized to access a certain area. Sharing of unique credentials is prohibited. Prior to granting an individual access to the work area(s), an assessment should be made to determine whether that person has a demonstrated need for access and has received authorization for access (refer to Chapter IX, Facility Access Determination).

*[Provide additional details about your facility’s access control systems that may include, but are not limited to: administrative controls such as lists of approved individuals and visitors; the use of personnel escorts; credentials such as photo identification badges for employees and visitor badges; electronic equipment such as badge readers, key pads that recognize unique codes, and biometric scanners; and keys.]*

* *What areas of the facility are secure area(s)? What separates the secure area(s) from other areas (e.g. a perimeter fence, gate, guards, secure doors)?*
* *Is the protection graded? Are there increasing layers of security at the facility based on proximity to VBM or other high-value/risk assets?*
* *Describe the access control system and the credentials required to enter each secure area (e.g., access rosters, escorts, badges, keys, codes, manual and electronic systems)*
* *What are the hours of operation? Do employees have access during specific times?*
* *Describe parking restrictions (Who is authorized to park vehicles on site? Are vehicle stickers or placards required? Is parking segregated form the building? How are deliveries and delivery vehicles handled?)*
* *How is the access control system maintained (e.g., periodic performance testing)?*
* *Describe the process for enrolling personnel in the access control system*
* *Describe the process for removing personnel from the access control system*
* *How is tailgating (person entering behind authorized personnel, with or without permission) prohibited to ensure each individual presents their own unique identifier for access?*
* *Describe visitor control and escorting procedures (Is there an approval process? Do visitors have designated parking? Are visitor logs used?)*
* *Describe the features of facility badges:*
  + *Are there different types of badges (e.g., employee, visitor, temporary)?*
  + *Do they have electronic access control (e.g., proximity, magnetic stripe)?*
  + *How long are badges valid?*
  + *When/where must badges be worn (e.g., administrative areas, biological work areas)?*

The use of keys and/or codes for access control is only effective when they are properly maintained and controlled. This can be accomplished through a Key Control Program and associated documentation (refer to Attachment G, Key and Code Control Form). *[Provide additional details about your facility’s key and code control program below, and/or reference the appropriate SOP(s)]*

* + *Who determines when to implement keys/codes?*
  + *Is there a dedicated Key Custodian/Control Officer responsible for the Key Control Program?*
  + *When are keys/codes changed? (e.g., loss or compromise, personnel changes)*
  + *Are keys inventoried? At what frequency?*
  + *Are keys returned/electronic access deactivated when an individual no longer requires access?*
  + *Does staff immediately report loss or theft of access credentials or keys?*
  1. Intrusion Detection

Intrusion detection notifies facility staff that an unauthorized individual has either attempted to enter or actually entered a restricted area. For low risk and administrative areas, abnormal observations such as a broken window or a secure door that is ajar may suffice, while facilities and areas with a higher potential for malicious conduct may choose to implement additional monitoring. Depending on the outcome of a comprehensive risk assessment, the facility may maintain one or more intrusion detection mechanisms to detect unauthorized access and activity. Intrusion detection systems typically consist of sensors (either automated or human), a mechanism to communicate to appropriate personnel that a sensor has been activated (alarms), and personnel who perform an assessment of the alarm to determine what response is required.

*[Provide additional details about your facility’s intrusion detection system(s) below]*

* *Describe the sensors used (e.g., trained guards, active or passive infrared motion detectors, magnetic switches, and glass break sensors)*
* *Describe the alarm system (e.g., how is it activated (unauthorized entry or movement), is it an audible and/or visual notification, does it automatically notify on/off-site guard forces and/or local law enforcement)?*
* *Does the system have a redundant power supply to ensure functionality during a power failure?*
* *How is the intrusion detection system maintained (e.g., reset process, periodic performance testing, battery replacement, sensor cleaning, firmware or software updates)?*
  1. Alarm Assessment and Response

Once an alarm has been communicated, an assessment should be performed by the guard force or other authorized personnel (such as local law enforcement personnel) to determine if the alarm is false or valid, and what actions, if any, are required to either interrupt the adversary or initiate an incident response protocol (refer to Chapter XXI, Emergency and Incident Response, Reporting and Investigation). Video surveillance refers to the monitoring of a designated area using a camera system. While constant monitoring of video surveillance is typically not the most effective a means of detection, it can be used to aid in alarm assessment and may also serve as a deterrent to unauthorized activity. The system may record all activity in the area for a defined period of time, which can be used to review events that occur in that timeframe. If the system does not have recording capability it may still be useful in real-time and alarm assessment.

*[Provide additional details about your facility’s alarm assessment and response procures below]*

* *Describe how responders perform an alarm assessment (by going to the site of the alarm to investigate, or remotely from a central alarm station equipped with appropriately configured communication and display system(s))*
* *Is a video surveillance system used? Are videos recorded? How long are they maintained? How is the video surveillance system maintained?*
* *Are results of alarm assessments documented? Is there an event log?*
* *Define roles and responsibilities during response (e.g., guard force, facility staff, management). Who responds to alarms and how are they trained? Is there a written response plan or procedures?*
* *Describe access delay measures to impede the progress of the adversary (e.g., guards, perimeter fencing, vehicle barriers, sturdy/locked doors, window bars, solid construction)*

In summary, all security measures should be implemented in a graded manner based on assessed biosecurity risks. Once a security system has been designed and implemented, management should ensure its successful operation through exercises, drills and self-assessments that cover: physical security, personnel management, MC&A, transport operations, and information security (refer to Chapter XXII, Biorisk Management System Assessment and Improvement).

1. Material Control & Accountability

When properly designed and implemented, inventory management systems can assist bioscience facilities in understanding, managing, optimizing, and securing flows of materials (including biological materials, reagents, consumables, supplies, etc.) into and out of the facility. An inventory management system will help enable the facility to monitor supply levels and order new supplies when needed while avoiding unnecessary costs or waste generation. An inventory system can deter or expose insider access to or removal of materials, as well as outsider threats. In addition to helping better manage facility resources and improve overall facility performance and efficiency (e.g., by helping to better control the quantities of various supplies maintained on site), the inventory helps form the basis for material control and accountability (MC&A) measures to help oversee the storage and use of biological agents and toxins, as well as other valuable biological materials. The primary objectives of MC&A are to establish internal oversight of biological agents and toxins, and to discourage theft and/or misuse.

Facilities that work with biological agents and/or toxins should develop a system to manage and oversee the inventory of these materials. This inventory may be integrated into a broader inventory of biological materials, reagents, supplies, and other property stored and used at the facility. A designated person should be assigned responsibility for overseeing the inventory system. The level of oversight and access control imposed on biological agents and toxins, and associated inventory information (such as storage locations, quantities, etc.), should be based on a risk assessment that includes consideration of both safety and security, as well as any applicable laws, regulations, or policies. *[List the applicable laws and/or regulations]*

The inventory in general, and particularly the inventory of biological agents and toxins, should therefore be current, complete, accurate, and updated regularly to account for changes in inventory levels. Those personnel assigned responsibility for assembling and/or maintaining the inventory should ensure the inventory information meets these basic conditions. In addition, accountability for materials can be assigned to knowledgeable individuals who work directly with the materials who can track and maintain inventory records and use to ensure materials are not orphaned or mishandled. Based on risk, the facility should determine and document what type and level of information should be captured for each item. *[List the specific information to be collected in the inventory system below, or reference the appropriate Valuable Biological Material Inventory Management Program Plan and SOPs]*

* *What specific criteria/data will be recorded, such as:*
  + *Name of agent/toxin*
  + *Characteristics (e.g., strain designation, GenBank Accession number)*
  + *Quantity acquired (e.g., containers, vials, tubes)*
  + *Initial and current quantity amount (e.g., milligrams, milliliters)*
  + *Date of acquisition*
  + *Source of acquisition*
  + *Storage location (e.g., building, room, and freezer)*
  + *When removed and/or returned from storage and by whom*
  + *Purpose of use*
  + *Transfer records (e.g., name and quantity of agent, date of transfer, name of sender and recipient)*
  + *Notification of theft, loss, or release records*
  + *Destruction records (e.g., name and quantity of agent, date, by whom)*
* *What training is provided to ensure compliance with the inventory management system?*
* *Who is responsible for MC&A (e.g., accountable individual for each item in the inventory: updates to the inventory system to include use, transfers and destruction)?*
* *What are the inventory reconciliation processes (e.g., frequency of auditing, reporting and resolving discrepancies)?*
* *How are materials handled and stored (e.g., appropriate temperature control, prevention of overcrowding, well organized, shelf-life management)?*
* *Are inventory locations minimized and provided adequate protection so that only authorized personnel have access (refer to Chapter XVI, Physical Security Systems)?*
* *How is information protected (refer to Chapter XVII, Information Control)?*
* *How are materials from suppliers validated?*
* *Are materials clearly labeled and tracked?*

1. Transportation and Shipping

When not properly packaged or contained, infectious substances can pose both a safety and security hazard to the public when transported outside of the facility. Many countries have strict regulations that govern the transport of infectious substances on roadways, through the air and in other public venues. There are also international regulations and standards that apply when transporting materials across international borders. If local or city regulations regarding shipment of infectious substances exist, a risk assessment of the material being shipped should be performed and considerations for packaging should made in accordance with nationally or internationally accepted practices. There may also be additional requirements to consider if using a refrigerant, like dry ice. In addition, most airlines follow strict international rules when accepting dangerous goods including infectious substances for transport. Fortunately, most countries, airlines and other carriers follow the same set of international guidelines published by the United Nations (UN) for the safe transport of dangerous goods. It is the policy of *[Insert Facility Name]* to strictly adhere to all applicable standards when transporting infectious substances both domestically and internationally, namely the WHO Guidance on Regulations for the Transport of Infectious Substances and International Air Transport Association (IATA) Dangerous Goods Regulations (DGR). Refer to the *Shipping and Transportation Program Plan Document XX* for additional information. General steps for shipping include:

* 1. Classify - determining whether your shipment is a regulated dangerous good or not; Category A, Category B, exempt human/animal specimen, etc.
  2. Identify - selecting a proper shipping name for your shipment. All dangerous goods must be assigned a proper shipping name and United Nations (UN) Identification number. These names and numbers are standard throughout the world.
  3. Package - infectious substances have specific packaging requirements that include a triple package concept: a leak-proof primary, leak-proof secondary, sufficient absorbent, and sturdy outer packaging.
  4. Mark and Label – proper marking and labeling helps identify the contents and describe the hazardous nature. The marks and labels required by international dangerous goods shipping regulations are the same in every country. Irrelevant marks and labels should be removed from any reused packaging.
  5. Document - several international standardized documents are designed to accompany shipments of dangerous goods. The following documents may be necessary for shipments depending on the dangerous good, the mode of transport, and the destination:
  + Shipper's declaration for dangerous goods
  + Pro-forma invoice listing details about the shipment, contents, number of packages, etc.
  + Air waybill
  + Import and/or export permits
  + For security purposes, a Memorandum of Understanding (MOU) may also be necessary to be completed and signed by both the sending organization and the receiving organization.

*[Cross reference other shipping and transportation documents or provide additional details about your facility’s specimen packaging and transportation procedures below (e.g., Transportation and Shipping Program Plan, Sample Collection Handbook), ensuring referenced documentation addresses the following security specific details]*

* *Describe the shipping functions at your facility (e.g., centralized (dedicated department), decentralized (trained individual users), or a risk-based hybrid)*
* *Describe training/certification required for individuals responsible for shipping*
* *List the personnel or department responsible for dangerous goods shipping*
* *Describe how security of samples is maintained throughout the shipping process (e.g., transport security procedures to be followed by sending, carrier and recipient entities)*
* *How are packages inspected (e.g., leaking, stained, odor, unusual, unexpected, odd size)?*
* *Where are packages brought and stored when first received? Is the area secured?*
* *How is material transported from reception to the biological work area(s)?*
* *Are employees trained to report suspicious packages? How are they reported?*

1. Information Security

Data, IT, and Cyber Security Systems

Information security is a set of tools and practices used to protect sensitive information that could be used for malicious intent. Protection of sensitive hard copy (paper) data will be achieved using lockable drawers and/or lockable file cabinets whenever approved individuals are not present. These keys will be managed within the Key Control Program (refer to Chapter XVI, Physical Security Systems). Passwords, networks, and internet accessible files are protected and not shared. Important electronic data is protected with network firewalls, unique passwords, encryption software, and computers physically secured.

*[Provide additional details about your facility’s information security policies and procedures below, and/or reference the appropriate SOP(s)]*

* *How is information determined to be sensitive? Is sensitive information marked or labeled? How is information reviewed and approved for public release?*
* *What information is sensitive at your facility (e.g., security-related information, inventories, floor plans, access rosters, laboratory notebooks and data)*
* *How is information security considered when screening and selecting hardware and software used in conjunction with assets, information, and people to be protected?*
* *Describe desktop/laptop security procedures*
* *Describe network security procedures and what elements are included in the network (e.g., routers, servers, Web servers and applications, domains, firewalls, wireless local area networks and remote access)*
* *Is there a secure server room? Are there stand-alone computers on isolated networks used within restricted areas?*
* *Describe how communication is controlled (e.g., encryption/ password protection)*
* *Are cell phones, cameras and other media storage devices limited or restricted?*
* *Is there centralized copying/ printing?*
* *How are hard copy (paper) and electronic files destroyed (e.g., shredding)?*

1. Personnel Reliability

The effectiveness of any procedure or process performed in a facility is ultimately determined by the training, capability, reliability, and integrity of its employees. Supporting personnel reliability is critical to the functioning of a facility by ensuring daily work practices and procedures are being performed by responsible and suitable personnel. Furthermore, personnel reliability procedures should consider whether personnel are physically capable of carrying out day-to-day activities in a manner appropriate for both safety and security concerns of the organization. The personnel reliability program helps to ensure that employees, who have access to critical items that could potentially be used for nefarious means, are reliable and trustworthy. Management is ultimately responsible for guaranteeing that its employees are adequately qualified and reliable to carry out the responsibilities of the position they hold. Security awareness is the knowledge and attitudes of the workers at all levels of an organization regarding the biological security concerns and appropriate responses to protect assets. Personnel must understand the importance of complying with security protocols (e.g. wearing badges, not propping open doors or bypassing physical security control measures, etc.). All requirements of a personnel reliability program should be consistent, transparent, and well-documented.

1. Personnel Reliability Program

The purpose of a personnel reliability program is to evaluate the suitability of a candidate before employment in a role having access to sensitive information, equipment, or materials and to ensure their continued suitability while employed. It is intended to identify individuals who may pose a biosecurity or biosafety risk as a result of a lack of trustworthiness, steadfastness or competency. A variety of medical, legal, ethical and psychological information about an individual can be used in the initial screening and verification, for ongoing monitoring, and to assess the importance of reportable derogatory information about, or potentially compromising situations involving, personnel. *[Reference applicable policy. Policy should state the conditions under which an individual would be found to be unreliable, whether adjudication of reliability is subject to appeal, and what employment and access actions are to be taken upon final adjudication. Refer to the Personnel Reliability SOP for additional information.]*

1. Initial and Ongoing Personnel Training

Successful completion of a range of biosecurity training programs may be required prior to accessing and/or performing activities in biological work areas. Please review Table 3 for information on the required trainings for staff or visitors that will be coordinated through the Biorisk Management Advisor.

|  |  |  |
| --- | --- | --- |
| *Table 3. Example Summary of Safety and Security Training* | | |
| ***Training*** | ***Requirement*** | ***Frequency*** |
| *Safe and Secure Operations* | *Prior to conducting activities in a work area* | *Annual* |
| *Respiratory Protection* | *Prior to wearing Respiratory Protection* | *Annual* |
| *Chemical Hygiene/ Hazard Communication* | *Within 120 days of hire* | *One time* |
| *[other training or topics as identified through risk assessment]* |  |  |

1. Succession Planning and Termination

A mechanism should be developed to ensure that the integrity of the facility will not be compromised through the absence of key individuals. Such a mechanism should include succession planning for management, scientific, technical and administrative personnel to ensure that critical knowledge of safe and secure operation of the facility does not reside with a single individual, in the event of his/her unavailability or departure. Documented procedures for dismissal of personnel and revoking access to the facility should be developed. Provisions describing personnel management should also address procedures and training for visitors, contractors, subcontractors, suppliers, and cleaning and maintenance staff.

*[Provide additional details about your Personnel Reliability program below, or write supporting SOP to be referenced]:*

* + *What types of job categories are considered low, medium or high risk? Is the authorization process more restrictive for high than that for low and moderate risk positions?*
  + *What is the minimum education requirement for individuals to have unescorted access to valuable biological materials (VBM), the existing physical security system, and/or the network infrastructure?*
  + *What should the screening process include (e.g., background check, verification of education and references) and what are the legal, technical, and financial limitations of this process?*
  + *Are there medical clearances and/or vaccination requirements/recommendations?*
  + *What training will be required prior to access and independent work? Is there a requirement for proficiency demonstration?*
  + *What behavior should be reported - security violations, criminal conduct, unexplained financial gain, unexplained absenteeism, degenerating physical appearance, insubordination/poor work performance, poor workplace relationships, alcohol/substance abuse, indications of excessive debt, excessive complaining?*
  + *What resources are available to employees suffering from adverse life events (e.g., Employee Assistance Program)*
  + *What are the consequences for violations?*
  + *Designate criteria to establish and maintain the suitability of individuals with access to VBM. How frequently are personnel re-assessed?*
  + *Designate criteria to establish temporary or permanent revocation of access to VBM for an individual due to medical restriction, suspension, disqualification, or administrative termination*
  + *What arrangements are made for short versus long-term visitors? Are they vetted prior to access?*
  + *What are the escorting procedures?*
  + *Describe procedures for maintaining redundancy and succession planning for critical operations*
  + *Describe termination procedures to ensure all access is revoked and materials are transferred (e.g., turn-in of keys, access cards, notebooks, and VBM, and de-activation of all electronic accounts)*

1. Access Determination

The purpose of the access determination process is to outline the security, medical, and training requirements for an individual to gain access to biological work areas or high safety/security risk agents at *[Insert Facility Name]* to ensure the safety and security of the facility’s operations and assets. Through this process personnel must successfully obtain the necessary clearances and approvals prior to being granted access. Documentation of the process is achieved using an Access Request *Form (refer to Biorisk Management Manual, Access Request Form Attachment)*. *[Provide additional details about your access determination process below, or write supporting SOP(s) to be referenced]*

* *Who authorizes access for the facility (and each biological work area) and on what basis?*
* *Who signs access determination forms and grants access (e.g., Scientific Manager/Director, Security Manager, Biorisk Management Advisor, Occupational Health)?*
* *Are there any access limitations in place for biological work areas versus administrative areas and are there increased access limitations in place for high risk areas (security operations center, sensitive information storage areas, containment areas, long-term sample storage/museums)?*
* *What are the access requirements for each secured area (e.g., training, medical, security)?*
* *What level of competency in security and safety procedures must individuals demonstrate prior to being granted unescorted access? How are access requirements verified?*
* *How are unapproved individuals allowed to conduct routine non-biological work (cleaning, maintenance, repairs)? Are they escorted and monitored always?*
* *How is access granted to accommodate long-term versus short-term visitors (academics, contractors, students, research fellows, visiting scientists, facility visitors, trades professionals, delivery personnel?*

Performance Checks, Reporting, Monitoring, Response, Review and Revision

The program assessment and performance measurement phases are an integral piece of the Plan-Do-Check-Act cycle without which there would be no assurance of program improvement. The following sections will address incident definition, reporting, and investigation; guide the establishment and review of performance metrics; ensure the implementation of competence reviews and drills from that may lead to corrective and preventive actions. These activities will facilitate the review of policy and management objectives, as well as organizational plans and assessments thereby creating as opportunity to make appropriate adjustments and communicate revisions.

1. Emergency and Incident Response, Reporting and Investigation
   1. Event Occurrence and Definition

Incidents can be small or large, and could require immediate action or may self-resolve. During the planning and preparation stages, a consensus must be reached to define an emergency and what differentiates a large incident from a small incident (refer to Emergency and Incident Planning). Events can also include breaches and potential breaches in the facility security program. *[Provide additional details about your facility’s definition of potential safety and security incidents and emergencies]*

* 1. Alert, Assessment, and Mobilization

The facility’s incident response plan should identify the individual(s) to alert after an incident occurs, or while it is occurring so that information can be used to initiate a response. The alert should occur simultaneously with an assessment of the type and severity of the incident that will also provide information to guide the response. For problems that require a response, mobilization is the activation of the personnel and equipment necessary to respond to the incident and resolve it quickly.

* 1. Response to Potentially Infectious Biological Release

All persons should immediately vacate the affected area and any exposed persons should be referred for medical advice coordinated through the facility’s occupational health program or external providers. The Scientific Manager and the Biorisk Management Advisor should be informed at once, and Security Manager involved if release is suspected to be intentional. If hostile adversary remains in the area, only appropriately trained Security personnel in personal protective equipment to mitigate all risks (safety and security) should enter the area to secure adversary. If spill/release is larger than *XX mL*, or inhalation hazard agent spills of any size, no one should enter the room for an appropriate amount of time (e.g. 1 h), to allow aerosols to be carried away and heavier particles to settle. If the work area does not have a central air exhaust system, entrance should be delayed (e.g. for 24 h). Signs should be posted indicating that entry is forbidden. After the appropriate time, decontamination should proceed, supervised by the biorisk management advisor. Appropriate protective clothing and/or respiratory protection should be worn, as needed for risks posed by agent involved in spill. *[Provide additional details about your facility’s emergency and spill response procedures below or reference the Spill SOP]*

* *What is the response to broken containers and spilled infectious substances?*
* *What is the response to a centrifuge accident or malfunction?*
* *What is the response to fire and natural disasters?*
* *Who is on the emergency contact roster for the facility?*
* *Who is the emergency service provider point of contact?*
* *What emergency equipment is made available on site (e.g., first aid kits, fire extinguishers, protective clothing, respiratory protection, disinfectants, tools)?*
* *Are there special response procedures for chemical, radiological or other hazards?*
* *Are personnel trained on how to respond to different alarms (e.g., evacuate, shelter in place)?*
* *Are security or emergency response personnel appropriately trained in PPE use for biological hazards? Do they have access to PPE appropriate for these risks?*
* *Have drills or exercises been performed periodically to practice, test, and evaluate response plans?*
  1. Incident Reporting, Investigation and Follow-up

Reporting and feedback are an important aspect of emergency and incident planning because it informs the planning and preparation stage and also provides information on what worked and where modifications/improvements are needed. Results from incident investigations should be used to update emergency response plans. Feedback can be obtained from the incident reports and questions (refer to Attachment H, Incident Response Form Template). *[Provide additional details about your facility’s incident investigation and follow-up procedures below]*

* + *What occurred leading up to the incident?*
  + *What steps were taken to reduce the impact of the incident?*
  + *Was there reasonable preparation to prevent the accident (e.g., was appropriate PPE or engineering controls used)?*
  + *Did detection occur promptly? If not, why?*
  + *Was the incident sufficiently contained?*
  + *Was communication adequate?*
  + *What issues were encountered during the response (e.g., expired supplies, insufficient PPE stocked, emergency systems not operating as expected)?*
  + *What opportunities for improvement were identified?*
  + *How are corrective measures implemented and evaluated?*
  + *Are there consequences for deliberate safety and security violations?*

1. Biorisk Management System Assessment and Improvement

Biorisk management systems are dynamic and require continuous assessment and flexible strategies to ensure ongoing and sustained improvement. Continuous quality improvement is a data driven management system that looks at processes/outcomes with key elements of accountability, good management, input from all levels of stakeholders, teamwork and continuous progress review in order to ensure safe environments and meet external standards and regulations. Biorisk management systems should use a continuous quality improvement approach like the “Plan-Do-Check-Act” approach as described in Principles.

* 1. Benefits of Performance Measurement

Measurement is the first step in the quality control and improvement process. It allows an organization to identify a baseline and understand the defects in the process which can be targeted for improvement. An organization receives many benefits from performance measurement such as:

* + Determining which parts of the BRM system are meeting stated goals or benchmarks
* Providing a demonstrable record of system performance
* Supporting facility certification/accreditation process
* Providing assurance that the risk is acceptable
* Facilitating maintenance and sustainability of the system
* Preserving resources by ensuring maximum efficiencies
* Helping to prevent incidents

Facilities may have several different systems that contribute to the effectiveness of biorisk management such as: testing and quality control, financial management, research results, general safety, and staff performance. The performance of these systems may be monitored to determine the overall performance of the BRM system. Biorisk management system performance refers to the way in which a biorisk management system actually functions to manage or minimize risk. Since actual biorisk management system performance may not match the planned level of risk management, performance measurements should be conducted to assess the differences between the expected and the observed. Biorisk management systems should undergo periodic review (Act portion of P-D-C-A) to ensure continued suitability, adequacy, and effectiveness. One essential tool is the reporting and analysis of facility inspection results *(refer to Biorisk Management Manual, Attachment I, WHO Laboratory Biosafety Manual, 3rd Edition, Part VII: Safety Checklist, which is not available with the 4th Edition of that publication). [Provide additional details about your facility’s management review process which should consist of analysis of data generated to measure performance such as:]*

* *Inspections, audits (describe frequency and scope)*
* *Monitoring records (e.g., equipment performance, quality control logs)*
* *Root-cause analysis of accident investigations (e.g., accident, injury, near-miss investigation data)*
* *Corrective and preventive actions*
* *Training programs*
* *Results of safety and security exercises and drills*
* *Data from surveys, questionnaires and employee feedback/observations*
* *Evaluation of improvements that have been implemented*

1. References
2. Centers for Disease Control and Prevention (CDC)/National Institutes of Health (NIH), Biosafety in Microbiological and Biomedical Laboratories (BMBL), 6th Edition, <https://www.cdc.gov/labs/BMBL.html>
3. ISO 35001 : 2019, Biorisk management for laboratories and other related organisations. <https://www.iso.org/standard/71293.html>
4. Salerno, RM and Gaudioso, J, Laboratory Biosecurity Handbook, CRC Press, Boca Raton, FL, 2007
5. World Health Organisation (WHO), Biorisk Management: Laboratory Biosecurity Guidance, September 2006, <http://www.who.int/csr/resources/publications/biosafety/WHO_CDS_EPR_2006_6.pdf>
6. WHO, Laboratory Biosafety Manual, 4th Edition, <https://www.who.int/publications/i/item/9789240011311>
7. Supporting Plans and SOPs
8. *Biorisk Management Manual*
9. *Operations and Maintenance Manual*
10. *Valuable Biological Materials (VBM) SOP*
11. *Shipping and Transportation Program Plan*
12. *Transport and Shipping Security SOP*
13. *Information Security SOP*
14. *Physical Security SOP*
15. *Personnel Reliability SOP*
16. *Material Control and Accountability SOP*
17. *Visitor Access SOP*
18. *Guard Force SOP*
19. *Emergency Response Plan*