Egypt. J. Chem. Environ. Health, 5 (2):1-19 (2019)
On line ISSN: 2536-9164

Laboratory Bio security risk assessment

By

Hanan, M. Sobhy and Ahmed M. Elmahdy

Biochemistry ,Toxicology & feed Deficiency Department, Animal Health Research Institute

ABSTRACT

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.

Definitions of biosecurity:

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.

Biohazard

The potential source of harm caused by biological agents or toxins.

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

 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

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.

Insider

Individual with authorized access.

Outsider

Individual without authorized access.

Adversary

Individual with malicious intent.

Asset

An item of value.

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.).

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).

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

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

Biosecurity risk assessment

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

When to Perform and Review a Laboratory Risk Assessment

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.

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
- . 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

Roles and Responsibilities for Risk Assessment(who should perform risk assessment)

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.

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:

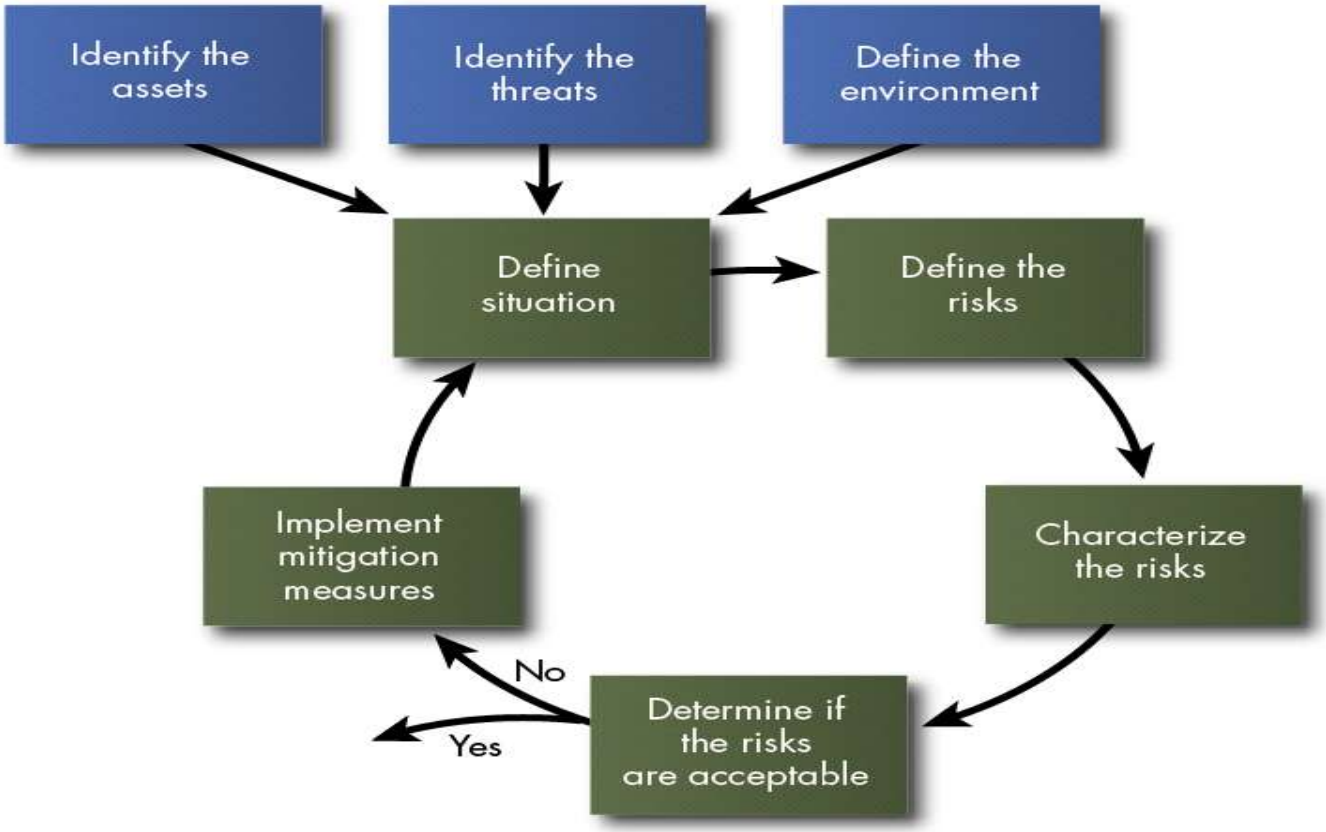
These individuals are directly affected by laboratory risks, often with limited knowledge about the hazards to which they are exposed. These individuals should be engaged regarding their concerns and understanding of the risks and how the results of the risk assessment will impact them. This is important 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.

Egypt. J. Chem. Environ. Health, 5 (2):1-19 (2019)
On line ISSN: 2536-9164

LABORATORY RISK ASSESSMENT METHODOLOGY



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.

1)Define the situation

- **Identify the assets**

The risk assessment team must identify and document the facility's assets that should be Protected 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.

- **Identify the threats**

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). 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

- **Define the facility and laboratory security 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.

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.

3) *Characterize the risks*

a) Asset Assessment

Based upon the defined risks, the risk assessment team should define ***the likelihood of targetingthe 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 and so on The team should likewise consider the consequences of a malicious use or destruction of the asset to both the facility and community (or environment).

b) **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.

c) **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:

1. **Physical Security**

 For long-term storage areas, what is the physical security situation of the asset?
o Is it secured? (e.g., is it in a locked freezer?)
o 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)?
o Is it secured? (e.g., is the room locked?)
o 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)?
o Is it secured?
o Is there any means to detect if an unauthorized person enters the building?
 What is the physical security situation of the facility or campus?
o Is it secured?
o 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? On site 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?

2. **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?

3. Material Control and Accountability

 Is information regarding the agent included in an inventory system?
o When is the agent included in the inventory system? Upon arrival?
Upon characterization?
o Is the inventory updated when the agent is disposed?
Does this inventory system include the name of a current accountable individual?
o 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?

4. Information Security

 What information is considered sensitive?
o Laboratory research data?
o Location and types of pathogens?
o Personnel identifying information?
 Would an adversary be interested in stealing or sabotaging this information?
 Is sensitive paper information secure?
o Is it physically secure?
 Is sensitive electronic information secure?
o Is information technology security in place? Are passwords used?
 Who has access to this data?

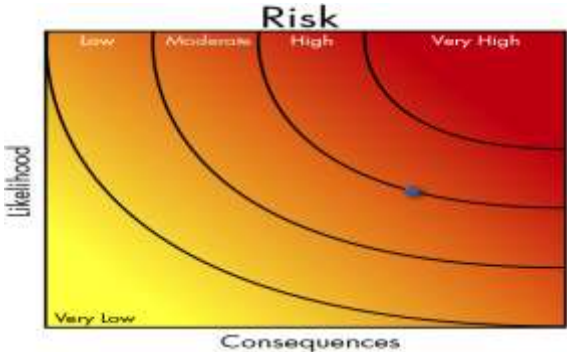
5. Transport security

 How often are samples transported to and from the lab?
 Who is involved in the transport process in your laboratory?
o Are the same individuals responsible for both packaging and receiving?
o Have they received adequate training in biosafety and biosecurity?
 How are the biological agents and toxins transported?
o Car? Bus? Plane?
 How are the biological agents and toxins stored en route?
o Is triple packaging used?
 Who is responsible for transporting the biological agents and toxins?
o Courier? Designated lab personnel?
o Have they received appropriate training in the event of a spill or
security incident?
 How are the biological agents and toxins secured between movements?
o Is chain of custody used?
o 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?

d) **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 a 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.



Overall risk graph

The blue dot represents the result of the risk characterization process showing a moderate to low likelihood and high consequences.

e) Risk assessment judgment

likelihood	consequences	Risk
Low	**Low**	**Very low**
Low	**Moderate**	**Very low to low**
Low	**High**	**low**
Moderate	**Low**	**Very low**
Moderate	**Moderate**	**Moderate**
Moderate	**High**	**High**
High	**Low**	**Low to moderate**
High	**Moderate**	**Moderate to high**
High	**High**	**Very high**

*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 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 Example

descriptionSituation	**Asset identification**
	Biological assets
	Asset no. 1 : biological samples containing hazardous pathogens (tuberculosis and brucella) and samples which brought by institute emergency missions for analysis and toxins (endotoxins and cigwa toxins) Current location: Sample Reception Unit **Impact to the facility from theft or destruction or misuse of the asset** financial impact ☒ reputational impact ☒ potential scientific/health impact ☒
	Description The financial impact is due to inability to perform the required analysis as a result for disappearance of the sample ,the reputational impact is due to inability to perform the required tests and scientific impact due to inability to certify customer food as safe which will make them loss money and inability of the customers to take decision of treatment to their living animal herds which will maximize their losses ,the health impact is due to the threat of using technology in isolating and multiplication of hazardous pathogens and toxins from samples and using them against community.

	Other assets
	Asset no. 2: Refrigerator Current location: Sample Reception Unit **Impact to the facility from theft or destruction or misuse of the asset** financial impact ☒ reputational impact ☒ potential scientific/health impact ☒
	Description Financial impact is due to the replacement cost of the refrigerator which equal to 10000 LE and the cost of calibration which equals to 200 LE , reputational impact is due to inability to receive and store the coming sample till analysis which may lead to refusing the samples , scientific impact due to inability to certify customer food as safe which will make them loss money and inability of the customers to take decision of treatment to their living animal herds which will maximize their losses
	Asset no. 3 : data entry computers Current location: data entry section at Sample Reception Unit **Impact to the facility from theft or destruction or misuse of the asset** financial impact ☒ reputational impact ☒ potential scientific impact ☐
	Description The financial impact is due to the replacement cost of these computers which equal 3500 LE for each computer ,reputational impact is due to the inability of the institute to issue the customers results on expected time due to the failure in samples data entry
	Asset no. 4: equipment used for further samples preparation(lamina air flow and flame) Current location: samples further processing section **Impact to the facility from theft or destruction or misuse of the asset** impact to the facility from theft or destruction or misuse of the asset financial impact ☒ reputational impact ☐ potential scientific impact ☐
	Description The financial impact is due to the replacement cost of the lab equipment
	Threats identification
	Adversary type
	Insiders Outsiders • Criminals ☐ ☒ • Competitive researchers ☐

	☒ • Criminals looking for items to sell ☐ ☐ • Disgruntled employees ☒ ☐ • A terrorist organization ☐ ☒ • Animal rights activists ☐ ☐
	Adversarial motivations to target these assets
	• financial gain ☒ • desire to destroy proprietary information ☐ • cause a nuisance by damage or destruction ☒ • inflict casualties ☐ • spread fear ☐ • make a political statement ☐ • protest ☐ • disgruntlement ☒
	Comment The adversary here may be outsider criminals with financial gain motivation stealing the SRU equipment, Disgruntled employees with disgruntlement motivation and a terrorist organization with desire to destroy proprietary information & cause a nuisance by damage or destruction. So the adversary here will be divided into • Insider Adversary – laboratory personnel motivated by disgruntlement. • Outsider Adversary – criminals looking to sell lab equipment, any potential terrorist organizations in the area
	Facility &laboratory security environment
	<u>vulnerabilities of the facility housing the assets:</u> The whole perimeter of the institute is +5 meters iron fenced with a +5 meters iron gates and the distance between the outer fences and the building of the institute is +15 meters which is used as a park for employees cars and guarded with 2 workers and monitored with CCTV during working hours and the gates were closed during off- working hours, the institute mainly contains 2 entrance points always guarded with security guards and CCTV during working hours the guards always collect the ID of the visitors before

	entering the institute and examine the employees by visual inspection during enter the gate , the iron gates of the entrance points were closed during off - working hours, the main building of the institute overlook the main street but all the windows of the ground floor in the institute is made of security glass and covered with iron bars. The institute entrance which leads to SRU has been made of strong wood and iron bars and closed with a non-reproducible keys lock and when the door is being opened during working hours it is always protected with a security guard (but no CCTV) ,the door of SRU is also made of strong wood and closed with a reproducible keys lock during off work hours ,the SRU is connected with the institute with an always closed door (opened only when samples were delivered to laboratories). **work being performed in the laboratory:** • Inspection, Registration and delivery of samples (which won't need any further preparation) to lab representative. • Inspection, Registration, preparation of samples (which will need further preparation) and delivery of samples to lab representative. • Samples automatic data entry **who has access to the laboratory and its assets** SRU staff personnel only during working hours Supervisor has master keys and authorized access .the lab. Supervisor has authority to issue keys to authorized personnel ,
	Physical Security **Asset security** : refrigerator is not locked or protected by any means of protection , the partition that contains lamina and flame closed by sliding door without any locks **Room security**: the lab staff are the only persons who permitted to enter the lab during working hours, The lab is locked (reproducible key lock) when not in use (off working hours). Only head of security team has a spare key **Building security**: There is an after-hour guard. Maintenance staff has Access . **Perimeter security** : Strong security fenced perimeter with closed CCTV monitored strong gates and security lab glass with additional iron bars protection **Personnel Reliability**: Lab personnel are not formally screened prior to laboratory access, but only examined by eye inspection of the security guards, no regular background checks or formal on-going behavioral assessments, annually formal governmental behavioral assessments have been documented. **Information Security** : Staff didn't receive any training on information protection or biosecurity but the SRU computers are multileveled password protected **Material Control and Accountability** : Staff receive introductory inventory management training **Transport Security** : No information is given
	• **Risk of an authorized person destroy VEM or VBM**

	laboratory personnel upset with management over issues concerning money or days off or penalties applied to them as a result of coming to the work late • **Risk of an unauthorized person stealing valuable biological material for personal gain , cause a nuisance** any potential terrorist organizations in the area intending to steal and sell a biological material or toxins • **Risk of an unauthorized person stealing equipment** Criminals may attempt to acquire SRU computer or equipment motivated by financial gain desire by break into the SRU overnight and during off working days
Characterize the risks	**Asset Assessment**
	Considering the assets, what is its likelihood of targeting the asset by the Threat? HIGH? MODERATE? LOW? - HIGH for the disgruntled workers. - MODERATE for other laboratory personnel (insiders) -LOW for outsiders **What would the consequences be of a misuse of the asset?** - Destruction / theft of equipment - high -Malicious release of hazardous pathogens of institute missions – high -Accidental exposure due to theft of Equipment contaminated with hazardous pathogens – high -Loss of samples data &work information details – LOW
	Adversary Assessment
	Insiders: not likely to consider hazardous pathogens for misuse toward the public, but more likely to damage equipment as disgruntled behavior. Outsiders: likely to consider stealing hazardous pathogens and toxins for misuse toward the public and make nuisance or steal equipment and other items of value.
	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 refrigerator and sliding door of partition containing further processing equipment are not locked at all, lab doors only locked after hours, access to all laboratory staff and maintenance crews, if necessary Aand the SRU entrance is not securely protected. **Personnel Reliability** – HIGH, due to lack of background checks and proper security training **Material Control and Accountability** – low due to high training and experience of staff working at SRU **Information Security** – low due to using of multileveled passwords

 Transport Security – unknown due to lack of information

risk	**Biosecurity event**	Asset	Adversary	LIKELIHOOD	**CONSEQUENCE**	**RISK LEEL**	**Risk ACCEPTANCE**
laboratory personnel upset with management over issues concerning money or days off or penalties applied to them as a result of coming to the work late	destruction	Refrigerator /lamina /flam / computers	Insider, Personnel	High	High for the institute	High	Not accepted
Any potential terrorist organizations in the area or criminal intending to steal and sell a biological material or toxins	Theft	Pathogens and toxins	Outsiders Terroristic groups	low	High Impacts to Public Health, high impact Animal Health, very high to institute (over all high consequences)	low	accepted
Criminals may attempt to acquire SRU computer or equipment motivated by financial gain desire by break into the SRU overnight and during off working days	Theft	Computer	Outsiders Criminal	low	low	Very low	accepted

Overall Risk Characterization

	Risk no 1 characterization is high
Determine if the risks are acceptable	*the risk isn't acceptable so special mitigation measures should be done to tolerate the risk and lowering them into acceptable level*
Implement risk mitigation measures	Mitigation measures for hazard no. 1 I think we should apply the following measures 1- Apply the lab cleaning process and the moving of the lab devices during cleaning under complete supervision of the lab staff member who is responsible for equipment record (recorded in document no. Housekeeping) 2- Monitoring of the lab devices with daily check annually calibrated devices (exp. Calibrated digital thermometer which monitoring annually calibrated refrigerator on daily time bases) and record the reading In document no. 3- Upon any unacceptable deviation from required performance of the lab equipment repairing and recalibration of the device should be applied immediately. **4- Apply access control to the SRU door.** The access control will help us to restrict the entrance of the SRU to authorized personnel and personnel who is given access permission by the authorized personnel during working hours and also used side by side with the SRU keys to close SRU door during off working hours.

Access control (outer panel) during experimental operation of the system

access control key

Access control (inner view)during experimental operation of the system

Access control power supply

Access control push button

5- Apply a lock to the refrigerator door and make a refrigerator records illustrating the samples in/out movement (sample accountability record).

Due to the purchasing unavailability of an external fridge and freezer lock at the Egyptian market

we submitted a recommendation for our institute TOP management for replacing the old SRU fridge with a new one containing a built in lock for fridge

Sample accountability record

6- All the aforementioned keys should be kept by the lab director and his deputy only.
7- Assign two of the young staff. Member who acquired the suitable characteristics (with direct contact with institute manager) to work as HR to receive any other member complain and help to solve any personnel problem
8- Apply an inner surveillance camera for monitoring the door of SRU and outer surveillance camera for monitoring the side exit of the institute which directly connected to the security office