Government of Canada / Gouvernement du Canada

CANADIAN BIOSAFETY GUIDELINE

CONDUCTING A BIOSECURITY RISK ASSESSMENT

Canada

The *Canadian Biosafety Guideline – Conducting a Biosecurity Risk Assessment* is available on the internet at the following address: https://www.canada.ca/en/public-health/services/canadian-biosafety-standards-guidelines/guidance.html

Également disponible en français sous le titre : *Effectuer une évaluation des risques de biosûreté*

To obtain additional copies, please contact:

Public Health Agency of Canada
100 Colonnade Road
Ottawa, ON K1A 0K9
Tel.: 613-957-1779
Fax.: 613-941-0596
PHAC email: PHAC.pathogens-pathogenes.ASPC@canada.ca

This publication can be made available in alternative formats upon request.

Publication date: Juin 2018

Catalogue Number: HP45-18/2018E-PDF
ISBN: 978-0-660-24518-8
Publication Number: 170397

TABLE OF CONTENTS

PREFACE

PREFACE

In Canada, facilities where Risk Group 2, 3, and 4 human pathogens or toxins are handled and stored are regulated by the Public Health Agency of Canada (PHAC) under the *Human Pathogens and Toxins Act* (HPTA) and the *Human Pathogens and Toxins Regulations* (HPTR). The importation of animal pathogens, infected animals, animal products or by-products (e.g., tissue, serum), or other substances that may carry an animal pathogen or parts thereof (e.g., toxin) are regulated by the PHAC or the Canadian Food Inspection Agency (CFIA) under the *Health of Animals Act* (HAA) and *Health of Animals Regulations* (HAR).

The following figure depicts the document hierarchy used by the PHAC and the CFIA to oversee their biosafety and biosecurity operations. Each tier of the pyramid corresponds to a document type, with documents increasing in order of precedence moving upwards. Acts and regulations are found at the top of the pyramid, as they are the documents that convey the PHAC's and CFIA's legal authorities. Guidance material and technical pieces are found at the bottom of the pyramid, as they are intended to summarize recommendations and scientific information only.

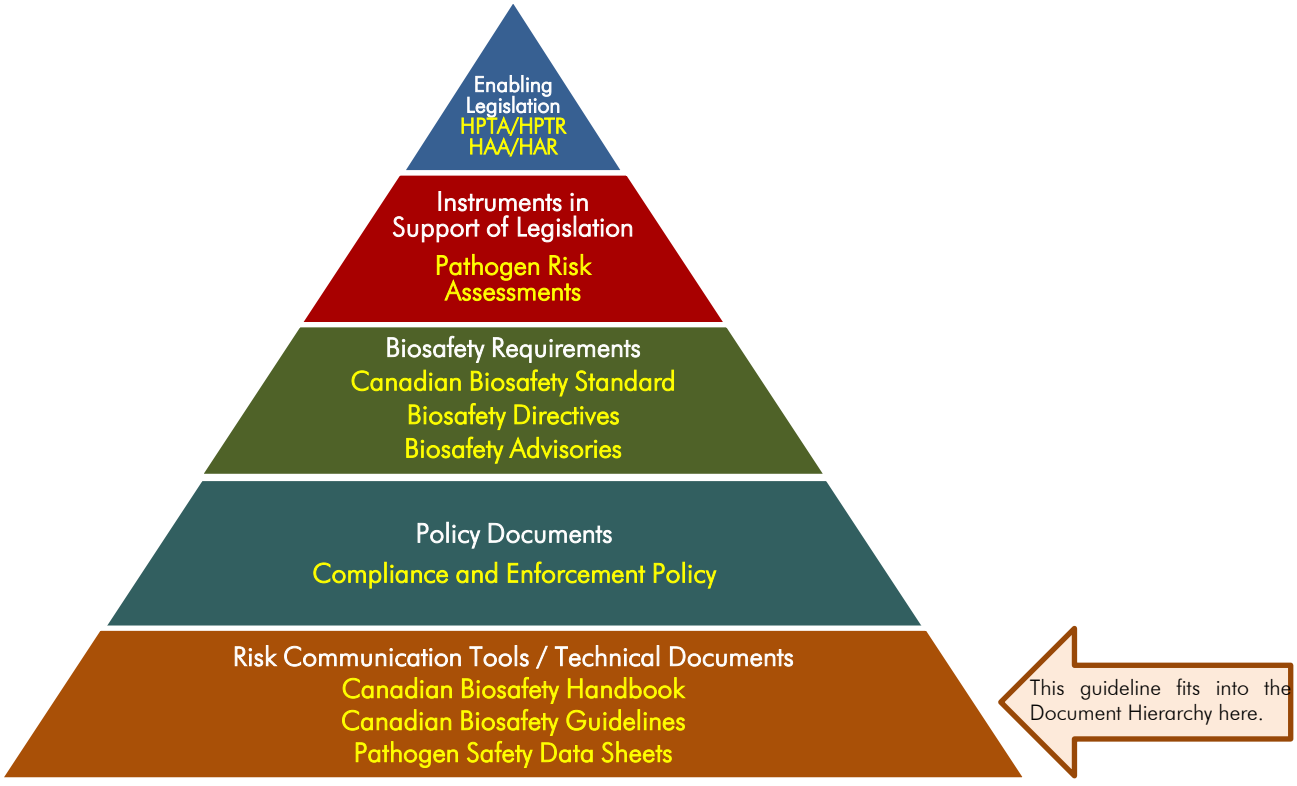


Figure 1: The Government of Canada's Biosafety and Biosecurity Document Hierarchy

This guidance document was developed by the PHAC and the CFIA as part of an ongoing series of electronic publications that expand upon the biosafety and biosecurity concepts discussed in the current edition of the *Canadian Biosafety Handbook* (CBH), the companion document to the *Canadian Biosafety Standard* (CBS). The *Conducting a Biosecurity Risk Assessment* guideline provides a methodology for assessment of biosecurity risks for facilities where human and animal pathogens and toxins are handled and stored. This guideline is intended to assist regulated parties in meeting the requirements specified in the CBS, but should not be interpreted as requirements. Regulated parties may choose alternate approaches to meet the requirements specified in the CBS.

Conducting a Biosecurity Risk Assessment is continuously evolving and subject to ongoing improvement. The PHAC and the CFIA welcome comments, clarifications, and suggestions for incorporation into the future versions. Please send this information (with references, where applicable) to:

PHAC e-mail: PHAC.pathogens-pathogenes.ASPC@canada.ca

ABBREVIATIONS AND ACRONYMS

ABBREVIATIONS AND ACRONYMS

CBH	*Canadian Biosafety Handbook*
CBS	*Canadian Biosafety Standard*
CFIA	Canadian Food Inspection Agency
IT	Information technology
PHAC	Public Health Agency of Canada
RG	Risk group (i.e., RG1, RG2, RG3, RG4)
SSBA	Security sensitive biological agent

CHAPTER 1

INTRODUCTION

CHAPTER 1 - INTRODUCTION

The words in **bold type** are defined in the glossary found in Chapter 10.

1.1 Purpose and Scope

This guideline, *Conducting a Biosecurity Risk Assessment*, proposes a methodology for conducting a **biosecurity risk assessment** by building on guidance introduced in Chapter 6 of the *Canadian Biosafety Handbook* (CBH) and other guidance found in domestic and international **risk** assessment methodologies.[1,2,3,4,5,6] Along with the *Canadian Biosafety Guideline: Developing a Comprehensive Biosecurity Plan*, it assists **facilities** in complying with **biosecurity** requirements in Canada.[7]

As specified in Matrix 4.1 of the *Canadian Biosafety Standard* (CBS), a biosecurity risk assessment must be completed in facilities where regulated **pathogens**, **toxins**, other regulated **infectious material**, and related **assets** are **handled or stored**.[8] The biosecurity risks associated with these materials are defined and appropriate mitigation strategies are determined to protect the materials and related assets from **biosecurity events** (i.e., theft, misuse, diversion, intentional unauthorized **release**, and accidental loss). Facilities may choose to develop a single biosecurity risk assessment at the organization level, or separate ones for individual locations or containment zones.

The information found in this guideline, including examples provided, is intended to provide a biosecurity risk assessment methodology. Many risk assessment techniques and methodologies exist and it is left to the organization to determine which methodology or technique is best for their particular situation.

A biosecurity risk assessment has unique considerations compared to **biosafety** and other risk assessments; however, the principles, concepts, and overall approach are quite similar. A biosecurity risk assessment, as described in this guideline, is concerned with biosecurity events that have the potential to cause adverse consequences to public health, animal health, or both, as well as to the organization. Additional information on biosafety and biosecurity can be found in the CBH.

The information and recommendations provided in the *Conducting a Biosecurity Risk Assessment* guideline are intended to be guidance and are not to be interpreted as requirements. Regulated parties may choose alternate approaches to meet the requirements specified in the CBS.

1.2 Overview

The handling and storing of pathogens and toxins poses a risk to public health, animal health, or both. Management of these risks necessitates an awareness and application of biosafety and biosecurity practices among personnel in laboratories and other containment zones where work with pathogens, toxins, infectious material, or infected animals is conducted.

To manage biosecurity risks, facilities are required to develop a **biosecurity plan** that addresses the risks identified in a biosecurity risk assessment. The complexity of the biosecurity plan is proportional to the risks posed by the compromise of an organization's assets. The biosecurity plan includes mitigation strategies for the risks associated with:

- physical security;
- personnel suitability and reliability;
- accountability for pathogens, toxins, and other regulated infectious material;
- **inventory**;
- **incident** and emergency response; and
- information management.

Risk is a function of the likelihood of an event occurring, and the consequences of that event, should it occur. Biosecurity event likelihood is determined by three factors: **adversary** motive, adversary capability, and historical frequency. Consequence is determined by two factors, impact and **vulnerability** (i.e., based on the effectiveness of **mitigation measures**), and assesses the severity of a biosecurity event. Effective mitigation measures within an organization seek to prevent, detect, respond to, and recover from biosecurity events and ultimately reduce risk. Weaknesses in mitigation measures (i.e., vulnerabilities) are addressed by improving the existing mitigation measures or implementing new ones.

Risk assessment can be highly subjective. Given that data on biosecurity events is limited and highly variable, this guideline recommends using the existing knowledge and expertise of personnel from within an organization by assembling a risk assessment team to collectively analyze the risks posed to an organization.

This guideline proposes a flexible and scalable approach for conducting a biosecurity risk assessment. Depending on a number of factors (e.g., complexity of an organization's activities, resources available, or fiscal and time constraints), it is left to the assessment team to determine the level of detail necessary for each activity within the biosecurity risk assessment process. This is achieved by aggregating biosecurity risk

assessment elements with similarities. With this in mind, it is recommended that elements of the biosecurity risk assessment follow a hierarchical structure, starting with a class, category, group, and individual, component, or event level. Conducting the biosecurity risk assessment at a group or category level will greatly reduce the workload and the complexity of the assessment, and should be considered unless there is reason to assess some elements on their own. Appendices B to E provide examples of risk assessment elements in their hierarchical structure.

Risk assessment is part of risk management and involves the following five steps:

1. Develop an asset inventory
2. Assess biosecurity event likelihood
3. Assess biosecurity event consequences
4. Analyze risk
5. Determine risk tolerance

Three additional activities common to risk management include: preparation, evaluation of vulnerabilities (i.e., based on the effectiveness of mitigation measures), and continual renewal and improvement. Table 1-1 provides an overview of how the steps outlined in this guideline relate to the risk management process presented in the CBH and the International Standards Organization (ISO) 31000 standard.[9]

Table 1-1: Relationship between the steps outlined in this guideline and those of ISO 31000 and the *Canadian Biosafety Handbook* (CBH)
The coloured rows highlight the different ways that the risk assessment step is broken down under each process.

ISO 31000		*Canadian Biosafety Handbook*	*Conducting a Biosecurity Risk Assessment* guideline
Establishing the Context		Preparation	Preparation
Risk Assessment	Risk Identification	Identify Assets, Consequences, Threats, and Vulnerabilities	Asset Inventory
			Likelihood
			Consequence
	Risk Analysis	Assess risk	Risk Analysis
	Risk Evaluation		Risk Tolerance
Risk Treatment		Mitigation	Mitigation
Monitoring and Review		Review and Continual Improvement	Review and Continual Improvement

As illustrated in Table 1-2, the components within this guideline are assessed using a scale of five values, including:

- very low (1);
- low (2);
- medium (3);
- high (4); and
- very high (5).

This scale is used to assess the priority of assets, likelihood of biosecurity events, severity of consequences, and risk level evaluation.

Table 1-2: Qualitative and quantitative component values[1]

Component Value (Quantitative)	1	2	3	4	5
Component Value (Qualitative)	Very Low	Low	Medium	High	Very High

This guideline uses key terms to assess component values, such as "very low" to "very high", "very infrequent" to "very frequent", "very low motivation" to "very motivated", "very limited" to "very sophisticated", and "negligible" to "widespread". It is left to the organization to define the meaning of these key terms.

1.3 How to use the Canadian Biosafety Guideline: *Conducting a Biosecurity Risk Assessment*

A detailed list of all abbreviations and acronyms used throughout this guideline is located at the beginning of the document; each word or term is spelled out upon first use, with the abbreviation immediately following in brackets and the abbreviation is used exclusively throughout the remainder of the document. A comprehensive glossary of definitions for technical terms is located in Chapter 10. Words defined in the glossary appear in **bold type** upon first use. Chapter 11 provides a list of the resources that were referenced in this guideline. In-text citations are listed in the references at the end of each chapter.

References

1 Government of Canada. (2016). *Canadian Biosafety Handbook* (2nd ed.). Ottawa, ON, Canada: Government of Canada. Available from https://www.canada.ca/en/public-health/services/canadian-biosafety-standards-guidelines/handbook-second-edition.html

2 Government of Canada, Communications Security Establishment, Royal Canadian Mounted Police. (2007). *Harmonized Threat and Risk Assessment Methodology, Version 1.0.* Ottawa, ON, Canada: Government of Canada. Retrieved 05/30, 2017 from https://www.cse-cst.gc.ca/en/publication/tra-1

3 Congressional Research Service. (2007). *The Department of Homeland Security Risk Assessment Methodology: Evolution, Issues, and Options for Congress.* Retrieved 05/30, 2017 from https://fas.org/sgp/crs/homesec/RL33858.pdf

4 Public Safety Canada. (2012). *All Hazards Risk Assessment: Methodology Guidelines, 2012-2013.* Ottawa, ON, Canada: Government of Canada. Retrieved 05/30, 2017 from https://www.publicsafety.gc.ca/cnt/mrgnc-mngmnt/mrgnc-prprdnss/ll-hzrds-rsk-ssssmnt-en.aspx

5 Salerno, R. M., & Gaudioso, J. (2007). *Laboratory Biosecurity Handbook.* Boca Raton, FL, USA: CRC Press.

6 Defence Research and Development Canada. (2017). *The Chemical, Biological, Radiological/Nuclear Explosive (CBRNE) Consolidated Risk Assessment (CRA) Rating Tool Guide.* Ottawa, ON, Canada: Government of Canada. Retrieved 05/30, 2017 from http://cradpdf.drdc-rddc.gc.ca/PDFS/unc262/p805090_A1b.pdf

7 Government of Canada. (2016). *Canadian Biosafety Guideline: Developing a Comprehensive Biosecurity Plan.* Ottawa, ON: Government of Canada. Available from https://www.canada.ca/en/public-health/services/canadian-biosafety-standards-guidelines/guidance/developing-comprehensive-biosecurity-plan-overview.html

8 Government of Canada. (2015). *Canadian Biosafety Standard* (2nd ed.). Ottawa, ON, Canada: Government of Canada. Available from https://www.canada.ca/en/public-health/services/canadian-biosafety-standards-guidelines/second-edition.html

9 *ISO 31000:2009, Risk Management – Principles and Guidelines.* (2009). Geneva, Switzerland: International Organization for Standardization.

CHAPTER 2

PREPARATION

CHAPTER 2 - PREPARATION

Preparation is an important preamble to biosecurity risk assessment. At minimum, it consists of gathering documentation, developing an understanding of the threat environment, defining scope, assembling an assessment team, and developing a risk assessment schedule.

2.1 Gathering Documentation

Documentation regarding organizational mandate, business plans, floor plans, program intent, overarching risk assessments, local risk assessments (LRA), pathogen risk assessments, Pathogen Safety Data Sheets (PSDS), and existing biosecurity risk assessments, along with any other relevant information, will be considered during the biosecurity risk assessment process and should be gathered beforehand.[1]

2.2 Threat Environment

Developing an understanding of the threat environment involves collating documentation and other information gathered from various sources and preparing a written overview of the current threat environment that may impact the organization. This activity should also venture beyond current and historical biosecurity events; it should take into consideration emerging biosecurity events that may become prevalent in the future as technology and the overall threat environment evolve. Remaining current on local, national, and international security and biosecurity events will lead to an enhanced understanding of the threat environment.

Consulting with relevant working units, such as the security department within larger organizations, will assist with this activity. Likewise, internal or external information technology (IT) security units, who are responsible for the security of computer systems and networks, may document cyber security incidents. These records will assist in the identification of potential biosecurity events and adversaries.

Local, provincial, and federal law enforcement agencies can be engaged to provide statistics related to criminal and suspicious activity in proximity to an organization's facility. Crime reports, crime heat maps, and access to online content can be requested from these agencies for biosecurity risk assessment purposes. Appendix A

provides a list of online resources with relevant information related to threats that may assist with this activity.

The scope of the biosecurity risk assessment should consider the organization's assets and potential relevant biosecurity events that are included in the assessment as well as indicate those that are excluded (e.g., natural disasters and technical failures).

2.3 Assessment Team

The assessment team should include individuals with in-depth knowledge of the organization's activities. The assessment team should also include an individual, often the biological safety officer (BSO), responsible for leading the biosecurity risk assessment; senior managers responsible for defining the risk tolerance of an organization; and other individuals who will contribute valuable knowledge throughout the biosecurity risk assessment (e.g., security specialists, scientists, laboratory personnel, human resources personnel, and IT personnel).

The composition of the assessment team should be tailored to match the complexity of the biosecurity risk assessment.

2.4 Schedule

A project plan outlining steps and timelines should be developed. The duration of the biosecurity risk assessment will depend on the complexity of an organization's activities, available resources, and fiscal and time constraints. The schedule should be sufficiently flexible to account for unexpected or unforeseen changes that may alter the risk or threat environments. The risk assessment project plan may include milestones, the person(s) responsible for each milestone, deadlines, expected duration of tasks, review periods, and approvals.

References

1 Government of Canada. Pathogen Safety Data Sheets. Available from https://www.canada.ca/en/public-health/services/laboratory-biosafety-biosecurity/pathogen-safety-data-sheets-risk-assessment.html

CHAPTER 3

ASSET INVENTORY

CHAPTER 3 - ASSET INVENTORY

3.1 Asset Identification

The asset inventory forms the foundation of a biosecurity risk assessment and leads to the implementation of adequate mitigation measures that aim to counter biosecurity events. Assets can be tangible, intangible, or people. A tangible asset can be described with physical properties (e.g., pathogens, toxins, equipment, animals, and hardware). Intangible assets do not have physical properties (e.g., scientific information, knowledge, biosecurity plan, logical processes, and even the reputation of the organization). People assets include individuals who play a key role in meeting the organization's mandate (e.g., personnel, students, contractors, senior managers, and scientists).

Careful attention should be given to assets that can be used for malicious purposes to cause disease in human or animal populations, or fear of such events. Such assets include those designated as security sensitive biological agents (SSBA), other human and animal pathogens and toxins, and assets with dual-use potential. The CBS requires that an inventory of regulated pathogens and toxins in long-term storage (i.e., greater than 30 days) be maintained (CBS Matrix 4.10).[1] Higher risk material (i.e., SSBAs, Risk Group 3 [RG3], and RG4) is required to be specifically identified. As indicated in the CBH, the quantity of pathogens, toxins, and related assets may be described in terms of a specific unit of measurement (e.g., number of vials or tubes, or mass amount), or they can be expressed with a range (e.g., number of animals in a colony [10-15]).[2] With this information, the potential for the intentional misuse of the pathogens or toxins can be identified and documented and the assets prioritized based on their qualities and the consequences of their compromise.

Pathogens and toxins with dual-use potential are of the greatest biosecurity concern. The human pathogens and toxins that have been determined to have a potential for misuse are referred to as SSBAs and identified in the *Human Pathogens and Toxins Regulations* (HPTR) as "prescribed pathogens" and "prescribed toxins".[3] In addition to pathogens and toxins, equipment and knowledge of potential dual-use should be identified. A decision tree for the identification of dual-use potential in life science research is included in the *Plan for Administrative Oversight for Pathogens and Toxins in a Research Setting – Required Elements and Guidance* and provides guidance on the identification of pathogens, toxins, and related assets, as well as knowledge with a potential for dual-use.[4] Good practice dictates that other factors, for example the concentration, quantity, and state of the material, also be included in the inventory.

Asset identification can be completed at an aggregated or component level (i.e., class, category, group, and individual or component). Animals can be identified at the group level (e.g., rat colony), rather than identifying each animal at the individual level. Conversely, pathogens and toxins can be identified at the component level (e.g., human immunodeficiency virus) rather than identifying those assets at a group level (e.g., RG3 pathogen or toxin, bacteria, virus, or parasite). Refer to Appendix B for an example list of assets, in their hierarchical structure, that can be included in a biosecurity asset inventory.

3.2 Asset Priority

Identifying an asset's qualities, coupled with the severity of consequences resulting from asset compromise, will help the assessment team establish asset priority. Prioritizing the asset inventory will then assist the team in establishing the mitigation measures required to protect the assets.

This guideline proposes that priority be established in an ordinal scale (e.g., 1 to 5, whereby a value of 5 is of very high priority and a value of 1 reflects an asset of very low priority) for every asset listed in the asset inventory. Refer to Table 3-1 for an example asset inventory.

Table 3-1: Example Biosecurity Asset Inventory

Asset Class	Asset Category	Asset Group	Component	SSBA	Risk Group	Quantity	State	Ease of Use	Location	Dual-Use Potential	Priority Value
Tangible	Biological	Virus	HIV	No	3	10 x 1ml tubes	Frozen	Difficult	Freezer A	No	Medium (3)
Intangible	Information	Inventory	Pathogen and Toxin Inventory	N/A	N/A	1	Electronic	N/A	N/A	N/A	High (4)
Tangible	Biological	Bacteria	*Bacillus anthracis*	Yes	3	5 x 1ml tubes	Frozen	Difficult	Freezer C	Yes	Very High (5)
Tangible	Biological	Bacteria	*Bacillus subtilis*	No	1	20 x 1ml tubes	Frozen	Difficult	Freezer C	No	Very Low (1)
Tangible	Equipment	Delivery System	Aerosolizer	N/A	N/A	1	N/A	Easy	Freezer C	Yes	Medium (3)
Intangible	Perception/ Reputation	Public Confidence	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Very High (5)
People	Employee	Scientist	Professor	N/A	N/A	20	N/A	N/A	N/A	Yes	Very High (5)

References

1 Government of Canada. (2015). *Canadian Biosafety Standard* (2nd ed.). Ottawa, ON, Canada: Government of Canada. Available from https://www.canada.ca/en/public-health/services/canadian-biosafety-standards-guidelines/second-edition.html

2 Government of Canada. (2016). *Canadian Biosafety Handbook* (2nd ed.). Ottawa, ON, Canada: Government of Canada. Available from https://www.canada.ca/en/public-health/services/canadian-biosafety-standards-guidelines/handbook-second-edition.html

3 *Human Pathogens and Toxins Regulations (SOR/2015-44).* (2015).

4 Government of Canada. (2015). *Plan for Administrative Oversight for Pathogens and Toxins in a Research Setting - Required Elements and Guidance.* Ottawa, ON, Canada. Retrieved 05/30, 2017 from https://www.canada.ca/en/public-health/services/laboratory-biosafety-biosecurity/licensing-program/plan-administrative-oversight-pathogens-toxins-a-research-setting-required-elements-guidance.html

CHAPTER 4

LIKELIHOOD

CHAPTER 4 - LIKELIHOOD

The Government of Canada defines a threat as "an event or act, deliberate or accidental, that could cause injury to people, information, assets, or services".[1] With this in mind, determining likelihood involves the identification of biosecurity events that have the potential to compromise assets possessed by an organization. Prior to starting this activity, reviewing the threat environment that was examined in the preparatory stage of the biosecurity risk assessment will help provide the context.

Biosecurity risk assessment focuses on identifying biosecurity events that include loss and events that are deliberate in nature (e.g., theft, misuse, diversion, and intentional unauthorized release).[2,3] All other unintentional events (e.g., accidents, earthquakes, hurricanes, or floods) may be considered in an all-hazards approach, but normally remain beyond the scope of the biosecurity risk assessment. Deliberate biosecurity events may be carried out by outsider or insider adversaries, who should be identified along with each biosecurity event.

The likelihood assessment involves the identification of deliberate biosecurity events, and determining adversary motive, means and capability, and historical frequency.

4.1 Biosecurity Event Identification

This activity includes the identification of biosecurity events that could result in unauthorized access, damage, loss, or misuse of an organization's assets. It is also important to consider the volatility of deliberate events, which can be carried out with little or no warning.[4] The focus of this activity should be on biosecurity event scenarios that seek to directly target the organization. These scenarios can be based on events that have happened locally or elsewhere (i.e., historical) or could possibly happen (i.e., hypothetical). Complex biosecurity event scenarios (e.g., those stemming from an indirect event) should not be included in this activity because the possible outcomes are difficult to determine.[4]

Deliberate biosecurity events can be carried out by physical means or through the use of cyber technology; the risk assessment team should consider both types of events.

It is left to the assessment team to determine the level of detail deemed necessary for this activity. The assessment team may decide to aggregate biosecurity events with similarities to reduce the complexity of the biosecurity risk assessment. This can be

achieved by classifying biosecurity events into a hierarchical structure (i.e., class, category, group, and individual event), as illustrated in Figure 4-1. This guideline recommends aggregating biosecurity events at most to the group level.

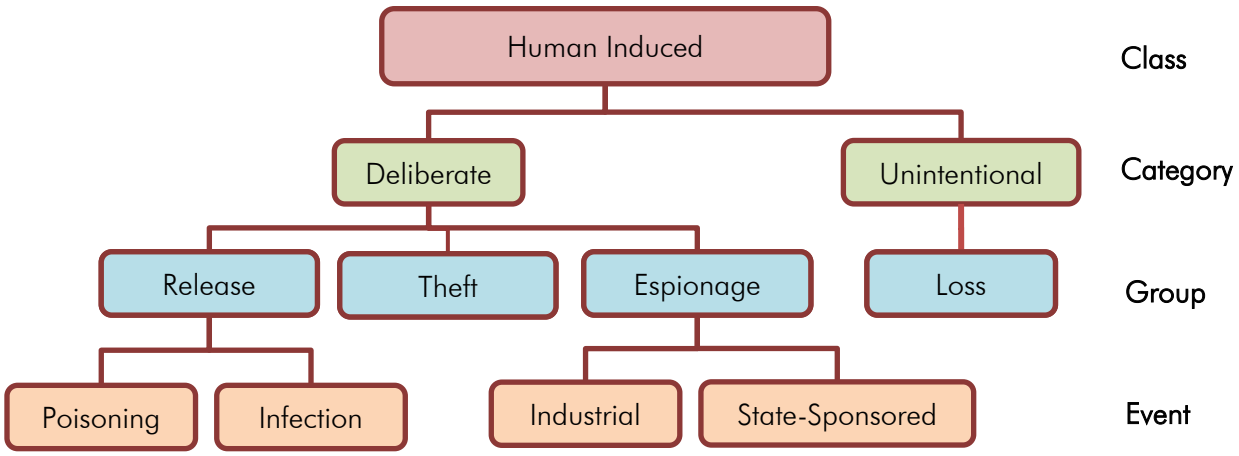


Figure 4-1: Biosecurity Event Hierarchy

4.2 Adversaries

Adversaries are individuals or groups that seek to deliberately compromise facility assets. Determining likelihood involves identifying adversaries (i.e., insiders and outsiders) that may have the motive, means, and capability to carry out a biosecurity event.[2,4,5] Opportunity exists when adversaries have the capability to exploit weaknesses in mitigation measures.

Insider adversaries, also known as insider threats, are individuals with authorized access to an organization's assets. Consideration should be given to disgruntled insider adversaries and the possibility for insider adversaries to be coerced, blackmailed, or rewarded to carry out a biosecurity event. Examples of insider adversaries may include personnel, contractors, students, and volunteers.

Outsider adversaries, also known as outsider threats, are individuals, organizations, or groups without authorized access to an organization's assets. Examples of outsider adversaries can include protesters, activists, former employees, visitors, opportunistic criminals, crime syndicates, lone actors, terrorist organizations, and radicalized individuals.

Adversary motive can be determined by expressed intentions of the adversary (e.g., employee telling others they will free the research animals) or from intelligence

suggesting an adversary's intention to carry out a biosecurity event. Such intelligence can be obtained from subject matter experts or by consulting external security agencies. Appendix A provides a list of online resources that may assist with this activity.

When assessing adversary motive, this guideline recommends using a scale of five values, as follows:

- Very low motivation (1)
- Low motivation (2)
- Somewhat motivated (3)
- Motivated (4)
- Very motivated (5)

Table 4-1 proposes the scales used for assessing adversary motive, means, and capability.

Similarly, adversary means and capability (e.g., ability to circumvent mitigation measures and to culture a pathogen or to extract a toxin) can be expressed in a scale with five categories, as follows:

- Very limited (1)
- Limited (2)
- Somewhat sophisticated (3)
- Sophisticated (4)
- Very sophisticated (5)

Adversary identification can be done at an aggregated level, by grouping adversaries with similar motives. It is recommended to conduct this activity by identifying adversaries in a hierarchical structure as presented in Appendix D. This guideline recommends aggregating biosecurity adversaries at most to the category level.

Table 4-1: Adversary Assessment

Motive	Motive Value	Means/Capability	Means/Capability Value
Very Motivated	Very High (5)	Very Sophisticated	Very High (5)
Motivated	High (4)	Sophisticated	High (4)
Somewhat Motivated	Medium (3)	Somewhat Sophisticated	Medium (3)
Low Motivation	Low (2)	Limited	Low (2)
Very Low Motivation	Very Low (1)	Very Limited/ None	Very Low (1)

4.3 Targeted Assets

Adversaries seek to target one or multiple assets when carrying out a biosecurity event. With this in mind, the assessment team should identify all assets that may be targeted.

4.4 Frequency

Assessment of likelihood considers the historical frequency of a biosecurity event. This can be done using available data, or it can be based on knowledge of employees and subject matter experts. The assessment team may find it useful to consult external agencies to collect data on frequency of biosecurity events. Appendix A provides a list of online resources that may assist with this activity.

The assessment team should consider biosecurity events and related security or criminal events (e.g., break and enter, vandalism, and sabotage) that have occurred in proximity to the organization's facility (i.e., the facility itself or similar local facilities external to the organization) and biosecurity events that have occurred at a distance from the facility (i.e., similar facilities at the regional, national, and global scale).

Table 4-2 proposes a frequency assessment scale for this activity. This table should be used with the assumption that biosecurity events in proximity to the organization's facility would indicate an increased likelihood of occurrence. Conversely, biosecurity events at distant locations would indicate a lower likelihood of occurrence.[4] Further consideration should be given to the frequency range of occurrence of biosecurity events (e.g., less than one month, one month to less than one year). It is

recommended that this table be customized to reflect the organization's particular situation.

Frequency in proximity and at a distance can be assessed with a scale with five values, as follows:

- Very infrequent/none (1)
- Infrequent (2)
- Somewhat frequent (3)
- Frequent (4)
- Very frequent (5)

Table 4-2: Biosecurity Event Frequency Assessment

Frequency Range	Proximity	Proximity Value	Distance	Distance Value
< 1 month	Very Frequent	Very High (5)	Very Frequent	Very High (5)
1 month < 1 year	Very Frequent	Very High (5)	Frequent	High (4)
1 year < 5 years	Frequent	High (4)	Somewhat Frequent	Medium (3)
5 years < 10 years	Somewhat Frequent	Medium (3)	Infrequent	Low (2)
10 years < 25 years	Infrequent	Low (2)	Very Infrequent	Very Low (1)
>= 25 years	Very Infrequent/None	Very Low (1)	Very Infrequent/None	Very Low (1)

4.5 Calculating Likelihood

To recap, the likelihood calculation involves identification of deliberate biosecurity events, and determining adversary motive, means and capability, and the historical frequency. Table 4-3 provides a likelihood calculation table that the assessment team can use to determine biosecurity event likelihood by assigning a value of one to five (i.e., 5 being very high, 1 being very low) for adversary motive, means and capability, and biosecurity event frequency. The likelihood value is an average of the four elements, rounded to the nearest whole number.

Table 4-3: Likelihood Assessment

Adversary		Frequency		Likelihood Value[a]
Motive	Means/Capability	Proximity	Distance	
Very Motivated (5)	Very Sophisticated (5)	Very Frequent (5)	Very Frequent (5)	Very High (5)
Motivated (4)	Sophisticated (4)	Frequent (4)	Frequent (4)	High (4)
Somewhat Motivated (3)	Somewhat Sophisticated (3)	Somewhat Frequent (3)	Somewhat Frequent (3)	Medium (3)
Low Motivation (2)	Limited Capabilities (2)	Infrequent (2)	Infrequent (2)	Low (2)
Very Low Motivation (1)	Very Limited Capabilities/None (1)	Very Infrequent/ None (1)	Very Infrequent/ None (1)	Very Low (1)

a) The likelihood value is an average of the four element values, rounded to the nearest whole number.

The following risk scenario demonstrates the use of the likelihood assessment table: An animal rights activist group that is very motivated with limited capability has carried out one deliberate release of infected animals in proximity to an organization's facility in the last fifteen years. In the last five years, they have carried out one deliberate release of infected animals from another facility in a distant region of the country.

Likelihood Assessment Example

Biosecurity event: deliberate release
Targeted asset: infected animal
Adversary: animal rights activist group

Motive = very motivated (very high 5)
Capability = very limited capabilities (very low 1)
Frequency (proximity) = infrequent (low 2)
Frequency (distance) = somewhat frequent (medium 3)

Likelihood = (motive + capability + proximity + distance)/4

= (very motivated + very limited capabilities + infrequent + somewhat frequent)/4

= (5 + 1 + 2 + 3)/4 = 11/4 = 2.75

Therefore, likelihood value is equal to 3 (rounded to the nearest whole number) or "medium".

Table 4-4 offers additional examples of biosecurity event likelihood assessments.

Table 4-4: Example Biosecurity Event Likelihood Assessment

Scenario	Biosecurity Event Category	Biosecurity Event Group	Adversary Class	Adversary Category	Adversary	Targeted Assets	Likelihood Assessment				
							Adversary Motive Value	Adversary Capabilities Value	Frequency (Proximity) Value	Frequency (Distance) Value	Likelihood Value[a]
Intentional release of infected animal by animal rights group	Deliberate	Intentional release	Outsider	Activist	Animal Rights Group	Animal	Very High (5)	Very Low (1)	Low (2)	Medium (3)	Medium (3)
Coerced insider commits theft of intangible information or technology	Deliberate	Theft	Insider	Contractor	Maintenance Personnel	Intangible Technology	Medium (3)	Very Low (1)	Low (2)	Low (2)	Low (2)
Disgruntled employee uses assets to infect personnel	Deliberate	Misuse	Insider	Personnel	Student	RG3 Pathogen and Toxin; Personnel	High (4)	High (4)	Very Low (1)	Medium (3)	Medium (3)

a) The likelihood value is an average of the four element values, rounded to the nearest whole number.

References

1 Government of Canada, Treasure Board Secretariat. (2012). *Policy on Government Security*. Retrieved 05/30, 2017 from https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578

2 Government of Canada. (2016). *Canadian Biosafety Handbook* (2nd ed.). Ottawa, ON, Canada: Government of Canada. Available from https://www.canada.ca/en/public-health/services/canadian-biosafety-standards-guidelines/handbook-second-edition.html

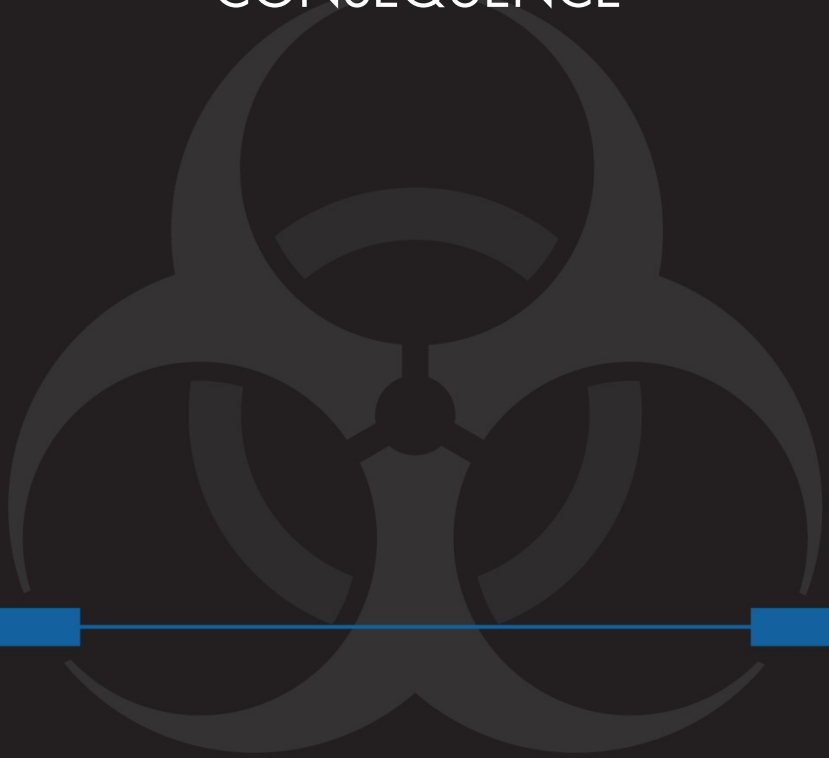
3 Salerno, R. M., & Gaudioso, J. (2007). *Laboratory Biosecurity Handbook*. Boca Raton, FL, USA: CRC Press.

4 Government of Canada, Communications Security Establishment, Royal Canadian Mounted Police. (2007). *Harmonized Threat and Risk Assessment Methodology, Version 1.0.* Ottawa, ON, Canada: Government of Canada. Retrieved 05/30, 2017 from https://www.cse-cst.gc.ca/en/publication/tra-1

5 United States Centers for Disease Control and Prevention, Division of Select Agents and Toxins & United States Animal and Plant Health Inspection Service, Agriculture Select Agent Program. (2013). *Security Guidance for Select Agent or Toxin Facilities (2nd Revision*). Retrieved 05/30, 2017 from http://www.selectagents.gov/resources/Security_Guidance_v3-English.pdf

CHAPTER 5

CONSEQUENCE



CHAPTER 5 - CONSEQUENCE

Biosecurity events can lead to death, disease, psychological impacts, and impacts to the organization. The severity of these consequences can be reduced with the implementation of effective mitigation measures. Furthermore, effective mitigation measures will enhance resilience and lead to a more rapid return to normal operations and steady state.

5.1 Impacts to Public Health, Animal Health, and the Organization

Biosecurity events can have physical and psychological impacts. Physical impacts could cause limited or widespread death or disease in human and animal populations. Psychological impacts could cause public fear. Biosecurity events can also result in a varying degree of impacts to the organization stemming from the loss of intellectual property and proprietary information, as well as costly response and recovery efforts.

Severe acute respiratory syndrome (SARS)[a], Ebola,[b] and bovine spongiform encephalopathy (BSE)[c] outbreaks, although not the result of deliberate actions, provide scenarios for assessment teams to consider when determining the severity of impacts resulting from the compromise of an organization's assets. These and other outbreaks have confirmed that in an increasingly interconnected world, biosafety and biosecurity events have the potential to cross geographic borders. Biosecurity events that last longer will result in increased costs of response and recovery; therefore, the local, regional, national, and global impacts should be taken into consideration when carrying out the impact assessment.

---

a The 2003 SARS outbreak, which began in an isolated farm in Asia, caused disease and loss of life globally, inlcuding some regions of Canada (e.g., the City of Toronto).

b The 2015 Ebola outbreak was mostly contained within Africa and caused disease and the death of thousands of people.

c In 2003, the BSE outbreak, also known as mad cow disease, in the UK resulted in the termination of 2,700 head of cattle.

Physical and psychological impacts on public health include the following criteria:

- Negligible or no disease and no death, or negligible public fear (1)
- Limited (one or few) cases of disease and no death, or limited public fear (2)
- Several localized cases of disease and minimal death, or some public fear (3)
- Widespread cases of disease and some death, or significant public fear (4)
- Widespread cases of disease and significant death, or widespread public fear (5)

Impacts to animal health include the following criteria:

- Negligible impacts in medium to high value livestock (1)
- Limited disease in medium to high value livestock (2)
- Some disease and potential for death in medium to high value livestock (3)
- Widespread disease and potential for death in medium to high value livestock (4)
- Widespread death in medium to high value livestock (5)

Impacts to the organization include the following criteria:

- Negligible financial costs associated with response and recovery efforts; Negligible loss of intellectual property, proprietary information, credit for research, or organizational reputation (1)
- Limited financial costs associated with response and recovery efforts; Limited loss of intellectual property, proprietary information, credit for research, or organizational reputation (2)
- Significant costs associated with response and recovery efforts; Significant loss of intellectual property, proprietary information, credit for research, or organizational reputation (3)

The main purpose of biosecurity is to prevent the loss, theft, misuse, diversion, or intentional release of pathogens, toxins, and other related assets in order to protect the health and safety of human and animal populations. The organization impact is included in the interest of the organization, to protect their assets and to produce a comprehensive risk assessment. Since organization impact, by definition, can only affect the organization, its maximum impact value is "medium" (3).

Impact to public health, animal health, and the organization can be expressed as a value ranging from 1 to 5, where 5 is very high and 1 is very low, as follows:

- Very low (1)
- Low (2)
- Medium (3)
- High (4)
- Very high (5)

The impact value is the highest of the three element assessed values (i.e., impact on public health, animal health, or the organization). For example, if a biosecurity event is assessed to have "medium" impacts to public health, "very low" impacts to animal health and "low" to the organization, then the impact value will be set to "medium" since it was the highest assessed value. A particular biosecurity event (e.g., espionage and sabotage) may not have any impact on public health and animal health; however, the impacts to an organization may be significant and result in significant loss of intellectual property, proprietary information, credit for research, reputation, and financial losses. This approach recognizes that a biosecurity event may not register with all three elements.

Table 5-1 provides an impact matrix and Table 5-2 provides additional examples that will assist with this activity.

Table 5-1: Impact Assessment

Public Health (Physical and/or Psychological)	Animal Health	Organization	Impact Value[b]
• Widespread cases of disease and significant death, or • Widespread public fear	• Widespread death in medium to high value livestock[a]	The maximum organization impact value is Medium (3)	Very High (5)
• Widespread cases of disease and some death, or • Significant public fear	• Widespread disease and potential for death in medium to high value livestock[a]	The maximum organization impact value is Medium (3)	High (4)
• Several localized cases of disease and minimal death, or • Some public fear	• Some disease and potential for death in medium to high value livestock[a] • Widespread death in other animals	• Significant to some financial costs associated with response and recovery efforts, or • Significant loss of intellectual property, proprietary information, credit for research, or organizational reputation	Medium (3)
• Limited (one or few) cases of disease and no death, or • Limited public fear	• Limited disease in medium to high value livestock[a] • Widespread disease and potential for death in other animals	• Limited financial costs associated with response and recovery efforts, or • Limited loss of intellectual property, proprietary information, credit for research, or organizational reputation	Low (2)
• Negligible or no disease and no death, or • Negligible public fear	• Negligible impacts in medium to high value livestock[a] • Some disease and potential for death in other animals	• Negligible financial costs associated with response and recovery efforts, or • Negligible loss of intellectual property, proprietary information, credit for research, or organizational reputation	Very Low (1)

a) The Canadian Food Inspection Agency (CFIA) has classified animals in terms of the economic value of the related industries to Canada as follows:

1. Highest value livestock industries: bovine, equine, porcine, poultry, crustaceans, finfish (wild and farmed).
2. Medium value livestock industries: small ruminants (sheep and goats), bees, molluscs, other farmed ruminants (cervids, bison).
3. Lowest value livestock industries and non-livestock animals: lagomorphs (rabbits), companion animals (dogs, cats, etc.), reptiles, amphibians, rodents, non-human primates.

b) The impact value is the highest of the three element values assessed.

Table 5-2: Impact Assessment

Scenario	Biosecurity Event Category	Biosecurity Event Group	Adversary Class	Adversary Category	Targeted Assets	Impact Assessment			
						Public Health Value	Animal Health Value	Organization Value	Impact Value[a]
Intentional release of infected animal by animal rights group	Deliberate	Release	Outsider	Activist	Animal	High (4)	High (4)	Medium (3)	High (4)
Coerced insider commits theft of intangible information or technology	Deliberate	Theft	Insider	Personnel	Intangible Technology	Not Applicable	Not Applicable	Medium (3)	Medium (3)
Disgruntled employee uses assets to infect personnel	Deliberate	Misuse	Insider	Personnel	RG3 Pathogen and Toxin; Personnel	Medium (3)	Medium (3)	Low (2)	Medium (3)

a) Impact value is the highest value of the previous three columns (public health, animal health, and organization impacts).

5.2 Vulnerabilities and Effectiveness of Mitigation Measures

Biosecurity risk assessment involves evaluating existing mitigation measures that exist within an organization to determine whether vulnerabilities (i.e., weak mitigation measures) exist that introduce opportunities for adversaries to carry out a biosecurity event.[1]

Effective mitigation measures can be implemented throughout all stages of incident management (i.e., prevention, detection, response, and recovery). Prevention aims to eliminate or reduce the risk of occurrence of a biosecurity event. Detection focuses on the early identification of a biosecurity event, allowing for prompt response. Response is the action taken during, or immediately before or after a biosecurity event to mitigate its consequences. Lastly, recovery includes the activities conducted to repair damages or restore conditions to an acceptable level after a biosecurity event has taken place.[2,3,4]

A mitigation measure can have one or multiple purposes in securing an organization's assets. The assessment of mitigation measure effectiveness is based on pre-biosecurity event (i.e., prevention) and post-biosecurity event (i.e., detection, response, and recovery) analysis, which is best guided by the assessment team's security specialists.[1]

A mitigation measure's effectiveness can be assessed by using a scale with five values, as follows:

- Very effective (1)
- Effective (2)
- Somewhat effective (3)
- Ineffective (4)
- Very ineffective or no mitigation measure (5)

The assessment team should assess each mitigation measure for its effectiveness pre-biosecurity event (i.e., prevention) and post-biosecurity event (i.e., detection, response, and recovery) at reducing the impacts of an event and then use the higher of the two values as the vulnerability value. For example, if security personnel is determined to be "effective" (i.e., "low" vulnerability [2]) during pre-event, and "somewhat effective" (i.e., "medium" vulnerability [3]) post event, the vulnerability value will be "medium" (3). A mitigation measure may not always be applicable during pre-biosecurity event or post-biosecurity event. In such instances, the vulnerability value is determined from the element to which a value has been assigned. Table 5-4 provides an example of mitigation measure assessment for an organization's security screening procedure. Table 5-3 can assist the assessment team with this activity.

Table 5-3: Vulnerability Assessment

Mitigation Measure Effectiveness		Vulnerability Value[a]
Pre-Biosecurity Event	Post-Biosecurity Event	
Not Applicable	Not Applicable	None
Very Ineffective or No Mitigation Measure	Very Ineffective or No Mitigation Measure	Very High (5)
Ineffective	Ineffective	High (4)
Somewhat Effective	Somewhat Effective	Medium (3)
Effective	Effective	Low (2)
Very Effective	Very Effective	Very Low (1)

a) The vulnerability value is the higher of the two element values assessed.

The output of this activity can take the form of a table. It begins with a listing of each existing mitigation measure at an aggregated level or component level. Identifying and aggregating mitigation measures follows a hierarchical structure, starting with a class, category, group, and component. The level of aggregation should be at the group or

component level; Table 5-4 provides an example output table for this assessment up to the group level. A mitigation measure will protect one or multiple assets; with this in mind, the assessment team should identify all assets that are being protected by a particular mitigation measure. Refer to Appendix E for an example list of biosecurity mitigation measures at the class, category, group, and component levels.

Table 5-4: Example of Vulnerability Assessment

Protected Asset(s)	Associated Biosecurity Event(s)	Mitigation Measure Class	Mitigation Measure Category	Mitigation Measure Group	Vulnerability Assessment		
					Pre-Biosecurity Event Value	Post-Biosecurity Event Value	Vulnerability Value[a]
Personnel, pathogens, toxins, infectious materials, prions, information, equipment	Theft, misuse, release, espionage, insider adversary	Security Program	Personnel Suitability	Security Screening	Low (2)	Not Applicable	Low (2)
Personnel, pathogens, toxins, infectious materials, prions, information, equipment	Theft, misuse, release, espionage, insider adversary	Security Program	Access Control	Security Guards	Very Low (1)	Low (2)	Low (2)
Personnel, pathogens, toxins, infectious materials, prions, information, equipment	Theft, misuse, release, espionage, insider adversary	Security Program	Training and Awareness	Insider Threat Training	Very High (5)	Not Applicable	Very High (5)
Equipment, pathogens, toxins, animals	Theft, loss, outsider and insider adversaries	Physical Security and Security Program	Access Control System	Entry and Exit Record	Very Low (1)	Very Low (1)	Very Low (1)
Personnel, pathogens, toxins, infectious materials, prions, information, equipment	Misuse, release, diversion, insider and outsider adversaries	Security Program	Emergency Response Plan	Release Recovery Procedure	Not Applicable	Low (2)	Low (2)

a) The vulnerability value is the higher of the two element values assessed.

5.3 Calculating Consequence

The consequence value is the product of the impact value multiplied by the vulnerability value. Table 5-5 combines impacts (Table 5-2) and vulnerability (Table 5-4) into one table and demonstrates how more than one mitigation measure can be applied to each impact.

Table 5-5: Example of Consequence Assessment

ASSET	Impact	Impact Value	Mitigation Measure	Vulnerability Value
Animals	High Public Health; High Animal Health; Medium to organization	High (4)	Access Control System	Very Low (1)
			Security Guards	Low (2)
Intangible Technology / Trade Secret	Medium to Organization	Medium (3)	Emergency Response Plan	Low (2)
			Insider Threat Training[a]	Very High (5)
RG3 Pathogen; Organizational Personnel	Medium to Public Health, Low to Organization	Medium (3)	Security Screening	Low (2)
			Insider Threat Training[a]	High (4)
			Access Control System	Very Low (1)

a) In this fictional example, insider threat training would be more effective at protecting RG3 pathogens and organizational personnel than technology and trade secrets.

References

1 Government of Canada. Communications Security Establishment, Royal Canadian Mounted Police. (2007). *Harmonized Threat and Risk Assessment Methodology Version 1.0.* Ottawa, ON, Canada: Government of Canada. Retrieved 05/30, 2017 from https://www.cse-cst.gc.ca/en/publication/tra-1

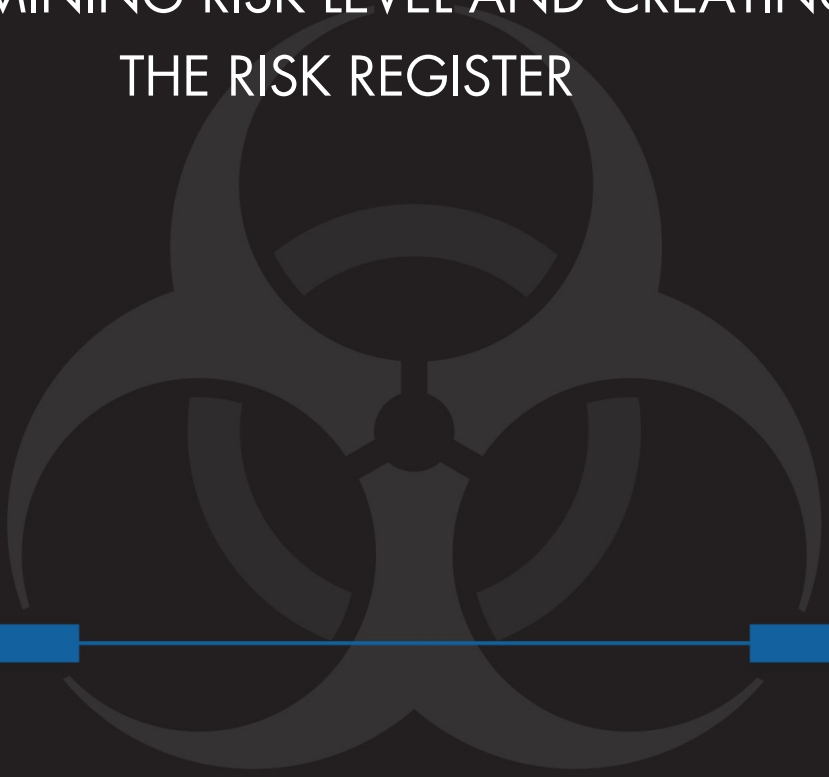
2 Public Safety Canada. (2017). *An Emergency Management Framework for Canada, Third Edition.* Ottawa, ON, Canada: Government of Canada. Retrieved 06/02 from https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2017-mrgnc-mngmnt-frmwrk/index-en.aspx

3 Public Safety Canada. (2013). *Building Resilience Against Terrorism: Canada's Counter-terrorism Strategy.* Ottawa, ON, Canada: Government of Canada. Retrieved 06/02 from https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/rslnc-gnst-trrrsm/index-en.aspx

4 Public Safety Canada. (2015). *Countering the Proliferation of Chemical, Biological, Radiological and Nuclear Weapons.* Ottawa, ON, Canada: Government of Canada. Retrieved 06/02 from https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cntr-trrrsm/cntr-prlfrtn/index-en.aspx

CHAPTER 6

DETERMINING RISK LEVEL AND CREATING THE RISK REGISTER



CHAPTER 6 - DETERMINING RISK LEVEL AND CREATING THE RISK REGISTER

The biosecurity risk level is based on an analysis of the risk associated with each asset (or group of assets with similar characteristics), which is a function of the likelihood of an event involving the asset, and the consequence of the event, should it occur. The highest biosecurity risks are those events with the greatest consequences, even if it is fairly unlikely they would occur, followed by events with moderate consequences that are more likely to occur.

This chapter will present the method for calculating biosecurity risk using the values determined in Chapters 3, 4, and 5, which addressed the evaluation of likelihood and consequences (and included consideration of existing mitigation measures) of biosecurity events.

6.1 Calculating Risk

The determination of biosecurity risk is based on analysis of each biosecurity risk scenario. To build risk scenarios, the results of all biosecurity event tables are combined into one output table. The risk is calculated by multiplying the likelihood value by the consequence values (i.e., impact and vulnerability) identified for each biosecurity risk scenario. The output of each risk calculation will result in a value ranging from 1 to 125. This range can be further divided into a group of five risk levels ranging from "very low" to "very high", as illustrated in Table 6-1. The risk calculation is presented in Section 6.2.

Table 6-1: Risk Level

Risk Range	1 – 4	5 – 18	19 – 34	35 – 74	75 – 125
Risk Level	Very Low	Low	Medium	High	Very High

6.2 Risk Register

A risk register is a common risk management tool that is used to document the results of risk analysis and risk response planning. It is a list of all risk scenarios and risk levels presented in a format that can be easily reviewed, modified, and updated. Table 6-2 illustrates a risk register that has been developed using the risk scenarios presented throughout this guideline.

Table 6-2: Risk Register

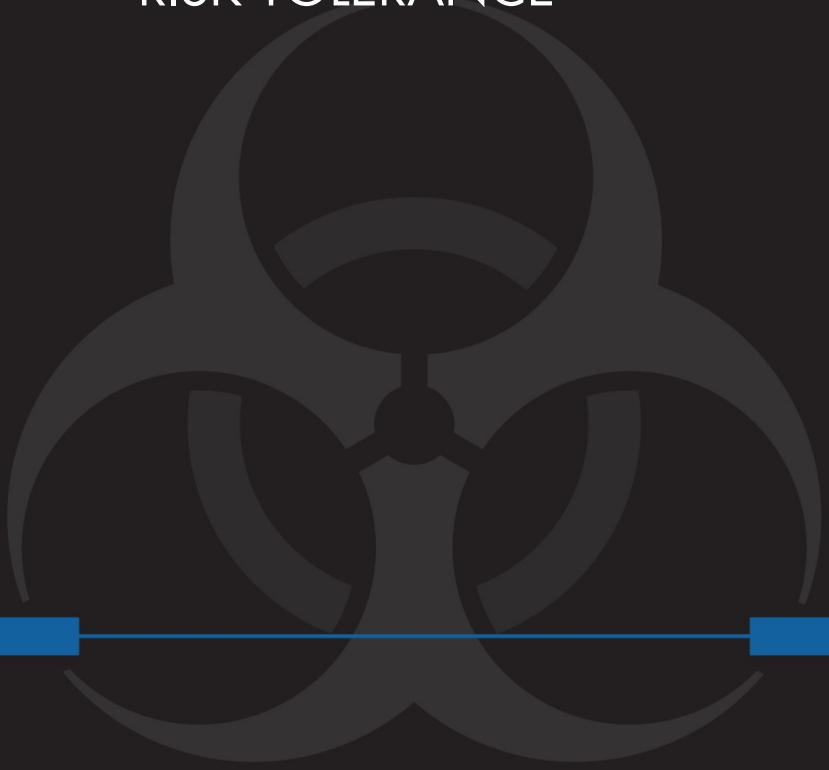
ASSET	LIKELIHOOD			CONSEQUENCE				RISK LEVEL[a]
	Biosecurity Event	Adversary	Likelihood Value	Impacts	Impact Value	Mitigation Measure	Vulnerability Value	
Animals	Release	Outsider, Activist	Medium (3)	High Public Health; High Animal Health; Medium to Organization	High (4)	Access Control System	Very Low (1)	Low (12)
						Security Guards	Low (2)	Medium (24)
Intangible Technology / Trade Secret	Theft	Insider, Personnel	Low (2)	Medium to Organization	Medium (3)	Emergency Response Plan	Low (2)	Low (12)
						Insider Threat Training	Very High (5)	Medium (30)
RG3 Pathogen; Organizational Personnel	Misuse	Insider, Personnel	Medium (3)	Medium to Public Health, Low to Organization	Medium (3)	Security Screening	Low (2)	Medium (18)
						Insider Threat Training[b]	High (4)	High (36)
						Access Control System	Very Low (1)	Low (9)

a) Risk Level is obtained by multiplying Likelihood Value, Impact Value, and Vulnerability Value.

b) In this fictional example, insider threat training would be more effective at protecting RG3 pathogens and organizational personnel than technology and trade secrets.

CHAPTER 7

RISK TOLERANCE



CHAPTER 7 - RISK TOLERANCE

Risk tolerance refers to the willingness of an organization to accept or reject a given level of **residual risk**, which is the remaining risk after assessment of mitigation measures.[1] Risk tolerance is based on the premise that zero risk is unachievable unless all potential threats are removed (e.g., activities with pathogens are no longer conducted).[2] Risk tolerance involves defining the organization's threshold or acceptable level of risk. **Senior management** is responsible for determining the acceptable level of residual risk for their organization, as well as ensuring that sufficient resources are available to mitigate risks deemed above the risk tolerance threshold.[2]

In Figure 7-1, the organization's risk tolerance threshold was set to "medium". The outcome of this decision flags risks that are considered to be "high" and "very high". Risks that exceed the risk tolerance threshold require the implementation of additional mitigating measures. The risk assessment team should identify new or enhanced mitigation measures, reassess the vulnerability value as described in section 5.2 and recalculate the risk as described in section 6.2 until it falls below the risk tolerance threshold. These results should be documented and shared with senior managers, as part of the mitigation measure recommendations, in the final risk assessment report.

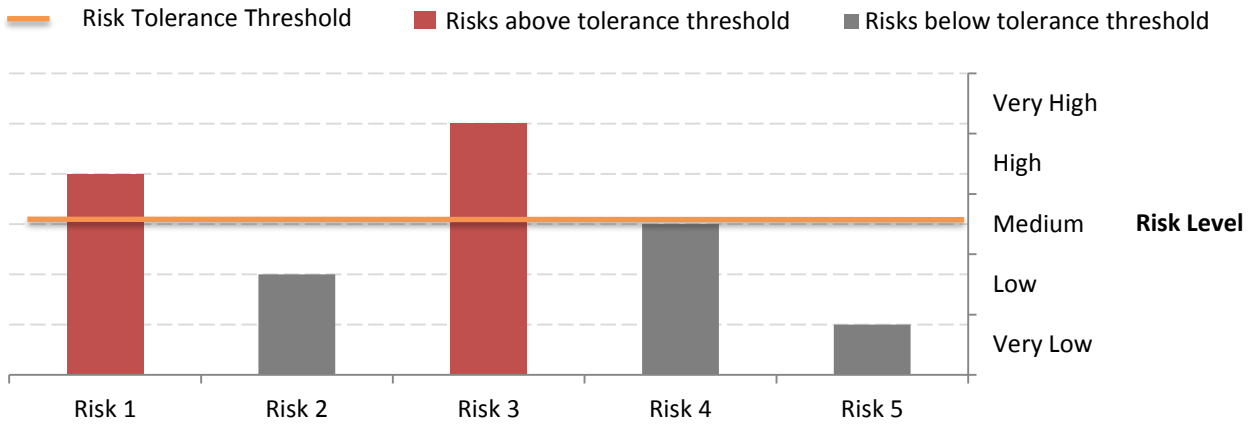


Figure 7-1: Risk Tolerance Threshold

Guided by the risk tolerance threshold, risks that register below the risk tolerance threshold are deemed acceptable. However, careful consideration should be given to risks that have been flagged at the low or high end of a risk level, as demonstrated in Table 7-1 for the item flagged with an "a", particularly given the subjectivity of input

values. For example, a risk determined to be medium may have registered with a score of 30, which is at the high end of the medium risk level (refer to Table 6-1). In this situation, senior management may choose to address this risk through mitigation measures even though it fell below the risk tolerance threshold. As a biosecurity program matures and more biosecurity risks are mitigated, the risk tolerance threshold may be gradually lowered in order to reduce an organization's overall risk level. The gradual lowering of risk level can be part of an organization's greater long-term strategy. Risk acceptance can be recorded within the risk register as an additional column, as shown in Table 7-1.

Table 7-1: Risk Register with Risk Acceptance Assessment

ASSET	LIKELIHOOD			CONSEQUENCE				RISK LEVEL	RISK ACCEPTANCE
	Biosecurity Event	Adversary	Likelihood Value	Impacts	Impact Value	Mitigation Measure	Vulnerability Value		
Animals	Release	Outsider, Activist	Medium (3)	High Public Health; High Animal Health; Medium to Organization	High (4)	Access Control System	Very Low (1)	Low (12)	Accepted
						Security Guards	Low (2)	Medium (24)	Accepted
Intangible Technology / Trade Secret	Theft	Insider, Personnel	Low (2)	Medium to Organization	Medium (3)	Emergency Management Response Plan	Low (2)	Low (12)	Accepted
						Insider Threat Training	Very High (5)	Medium (30)[a]	Not Accepted
RG3 Pathogen; Organizational Personnel	Misuse	Insider, Personnel	Medium (3)	Medium in Public Health, Low for Organization	Medium (3)	Security Screening	Low (2)	Medium (18)	Accepted
						Insider Threat Training[b]	High (4)	High (36)	Not Accepted
						Access Control System	Very Low (1)	Low (9)	Accepted

a) Risk at the high end of the medium risk level. Although the risk falls below the risk tolerance threshold, the decision was taken to mitigate it.

b) In this fictional example, insider threat training would be more effective at protecting RG3 pathogens and organizational personnel than technology and trade secrets.

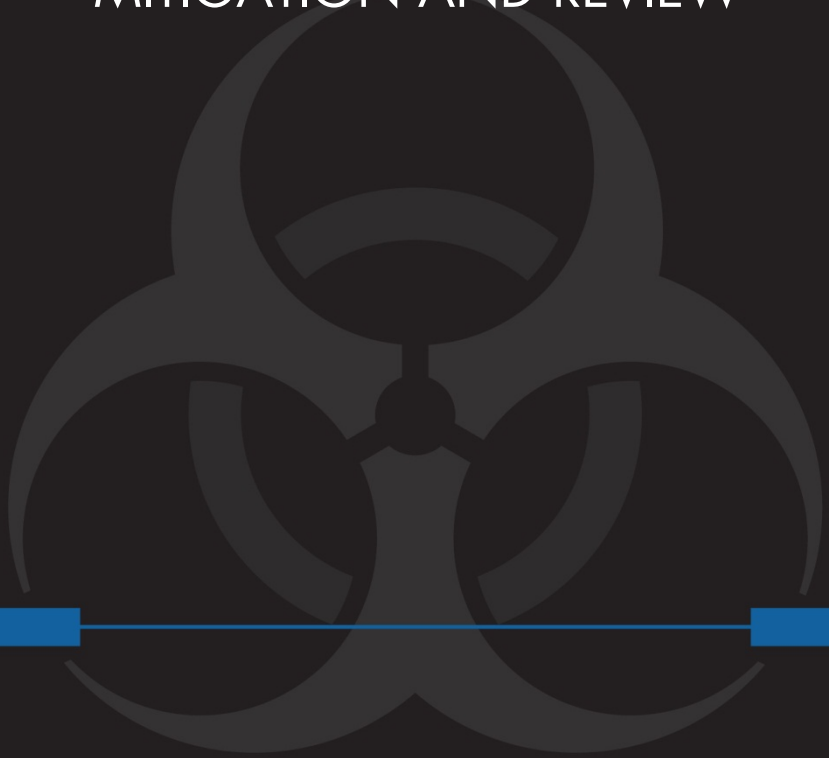
References

1 Public Safety Canada. (2012). *All Hazards Risk Assessment: Methodology Guidelines, 2012-2013*. Ottawa, ON, Canada: Government of Canada. Retrieved 05/30, 2017 from https://www.publicsafety.gc.ca/cnt/mrgnc-mngmnt/mrgnc-prprdnss/ll-hzrds-rsk-ssssmnt-en.aspx

2 Government of Canada. (2016). *Canadian Biosafety Handbook* (2nd ed.). Ottawa, ON, Canada: Government of Canada. Available from https://www.canada.ca/en/public-health/services/canadian-biosafety-standards-guidelines/handbook-second-edition.html

CHAPTER 8

MITIGATION AND REVIEW



CHAPTER 8 - MITIGATION AND REVIEW

8.1 Mitigation

The biosecurity risk assessment informs the biosecurity plan, which documents the mitigation measures put in place to address risks. Risks that fall outside of the risk tolerance threshold should be controlled through additional or enhanced mitigation measures. A cost-benefit analysis can assist in determining the mitigation measures in which to invest.

Financial constraints and resource limitations may present challenges when looking to manage unacceptable risks. As a starting point, senior management may choose to initially focus mitigation measures on the most consequential risks and then control remaining risks as resources become available. In other instances, if the risks are determined to be too high or costly to mitigate, the organization's project or program may need to be modified or cancelled.

Recommendations for mitigation measures should be documented in the final report of the biosecurity risk assessment. More information on mitigation measures can be found in the Canadian Biosafety Guideline *Developing a Comprehensive Biosecurity Plan*.[1]

8.2 Review

It is recommended that the biosecurity risk assessment be reviewed routinely and updated when necessary to address changes that would affect the level of risk (e.g., threat environment, regulation and policy, after a biosecurity event occurs, program renewal, newly discovered vulnerabilities, construction of a new facility, and additions or subtractions to an organization's asset inventory).[2]

References

1 Government of Canada. (2016). *Canadian Biosafety Guideline: Developing a Comprehensive Biosecurity Plan.* Ottawa, ON: Government of Canada. Available from https://www.canada.ca/en/public-health/services/canadian-biosafety-standards-guidelines/guidance/developing-comprehensive-biosecurity-plan-overview.html

2 Government of Canada. (2016). *Canadian Biosafety Handbook* (2nd ed.). Ottawa, ON, Canada: Government of Canada. Available from https://www.canada.ca/en/public-health/services/canadian-biosafety-standards-guidelines/handbook-second-edition.html

CHAPTER 9

REPORT FINDINGS

CHAPTER 9 - REPORT FINDINGS

Once the assessment is complete, the findings and recommendations to senior management and decision makers should be presented in a comprehensive biosecurity risk assessment report. The decision to prepare a biosecurity risk assessment report is optional and left to the discretion of the assessment team since the biosecurity risk assessment is complete; however, summarizing the findings and placing emphasis on higher risks will facilitate communication and understanding of the biosecurity risk assessment. The report should summarize the biosecurity risk assessment and present the scenarios of highest risk as well as recommendations for reducing unacceptable risks. This report and the biosecurity risk assessment itself may contain sensitive information and are considered assets to be evaluated in the risk assessment process.

The following ten sections are proposed for the biosecurity risk assessment report:

1. Executive Summary
2. Purpose
3. Scope
4. Background
5. Threat Environment
6. Asset Inventory
7. Risk Assessment Results
8. Risk Tolerance
9. Recommendations
10. Appendix:
    a) Asset Inventory
    b) Biosecurity Event Table
    c) Likelihood Table
    d) Consequence Table
    e) Risk Register
    f) Schedule
    g) Team members

9.1 Executive Summary

The executive summary should appear at the beginning of the report and should briefly discuss the purpose, scope, background, threat environment, risk scenarios with the highest risk, and recommended measures to mitigate those risks.

9.2 Purpose

At minimum, the purpose should consist of a short statement describing what the biosecurity risk assessment report intends to achieve. For example: "This report presents the findings of a biosecurity risk assessment conducted on Laboratory X and provides recommendations for mitigation measures for unacceptable risks".

9.3 Scope

At minimum, the scope should include the following elements:

- Site(s) included in the assessment
- Biosecurity events that were assessed and the time frame that was assessed (i.e., biosecurity events that were expected to persist in the short-term and long-term)
- Biosecurity events and time frame that were not assessed
- Asset class or group that falls within the scope of the assessment
- Asset class or group that falls outside the scope of the assessment

9.4 Background

The background is an integral part of the introductory section of the biosecurity risk assessment report. At minimum, this section should include the following elements:

- Organization's mandate
- Objectives of the organization
- Description of the reason why a biosecurity risk assessment is being performed or updated (e.g., new assets have been added, the threat environment has evolved, facility relocation)

9.5 Threat Environment

The threat environment profile that was developed in the preparation section of the biosecurity risk assessment can be modified to include any significant findings that were learned throughout the biosecurity risk assessment process. The threat environment section should document threats that are expected to persist in the short and long-term, as well as emerging threats.

9.6 Asset Inventory

The asset inventory describes the assets within the scope of the biosecurity risk assessment. At minimum, this section should summarize and identify assets that are most significant. All other assets that were identified should be documented in the Appendix.

9.7 Risk Assessment Results

The risk assessment results should focus on the risk scenarios that fell outside of the risk tolerance threshold. This section will benefit from graphical or tabular representation of the risk scenarios. A snippet of the risk register can be used as a visual aid.

9.8 Risk Tolerance

A short statement of the risk tolerance that was set by senior management should be included. At minimum, it should identify the risk tolerance threshold that was chosen to define the maximum level of acceptable risk and the rationale that led to the decision.

9.9 Recommendations

Recommendations will ultimately inform the organization's biosecurity plan; thus, this section should propose mitigation measures. At minimum, this section should:

- identify risk scenarios that fall outside of the risk tolerance threshold;
- identify inadequate mitigation measures that require further attention; and
- propose additional mitigation measures that will reduce the organization's risk level.

Recommendations can also include an estimate of the resources required to implement mitigation measures. In some cases, this may require financial expenditures or simply changes in security procedures, or additional training and awareness for personnel.

9.10 Appendix

The appendix expands on the summary information found in the biosecurity risk assessment report. At minimum, the appendix should contain all outputs developed throughout the risk assessment process, such as the following:

- Asset inventory
- Biosecurity event table
- Likelihood table
- Consequence table
- Risk register

The appendix can also include material that was prepared during the first step of the biosecurity risk assessment process, such as the following:

- Biosecurity risk assessment schedule
- Risk assessment team members

CHAPTER 10

GLOSSARY

CHAPTER 10 - GLOSSARY

It is important to note that while some of the definitions provided in the glossary are universally accepted, many of them were developed specifically for the CBS, the CBH, or the *Canadian Biosafety Guideline: Conducting a Biosecurity Risk Assessment*; therefore, some definitions may not be applicable to facilities that fall outside of the scope of the CBS.

Adversary (plural: Adversaries)	An individual, organization, or group that has the capabilities and motive to carry out a threat event. An adversary can be an insider or an outsider who acts alone or under the direction of an organization or state.
Assets (singular: asset)	All of the pathogens, infectious material, toxins, and related resources in the possession of a facility, including materials, equipment, non-infectious biological material, animals, knowledge and information (e.g., protocols, research findings), and personnel in a facility.
Biosafety	Containment principles, technologies, and practices that are implemented to prevent unintentional exposure to pathogens or toxins, or their accidental release.
Biosecurity	Security measures implemented to prevent the loss, theft, misuse, diversion, or intentional release of a human pathogen, toxin, and other related assets (e.g., personnel, equipment, non-infectious material, and animals).
Biosecurity event	A deliberate act involving or related to pathogens or toxins, information, or equipment that could cause disease or harm to people, animals, or both, as well as to the organization.
Biosecurity plan	Plan for the implementation of mitigation strategies for the risks associated with: physical security; personnel suitability and reliability; accountability for pathogens, toxins, and other regulated infectious material; inventory; incident and emergency response; and information management.
Biosecurity risk assessment	A risk assessment in which the pathogens, toxins, infectious material, and other related assets (e.g., equipment, animals, information) in possession are identified and prioritized, the threats and risks associated with these materials are defined, and appropriate mitigation strategies are determined to protect these materials against potential theft, misuse, diversion, or intentional release.
Disease	A disorder of structure or function in a living human or animal, or one of its parts resulting from infection or intoxication. It is typically manifested by distinguishing signs and symptoms.
Dual-use potential	Qualities of a pathogen or toxin, knowledge, or equipment that allow it to be either used for legitimate scientific applications (e.g., commercial, medical, or research purposes), or intentionally misused as a biological weapon to cause harm (e.g., bioterrorism).
Facility (plural: facilities)	Structures or buildings, or defined areas within structures or buildings, where infectious material or toxins are handled or stored. This could include individual research and diagnostic laboratories, large scale production areas, or animal housing zones. A facility could also be a suite or building containing more than one of these areas.

Handling or storing	Possessing, handling, using, producing, storing, permitting access to, transferring, importing, exporting, releasing, disposing of, or abandoning pathogens, toxins, or infectious material. Includes all controlled activities involving human pathogens and toxins specified in Section 7(1) of the *Human Pathogens and Toxins Act*.
Incident	An event or occurrence with the potential of causing injury, harm, infection, intoxication, disease, or damage. Incidents can involve infectious material, infected animals, or toxins, including a spill, exposure, release of infectious material or toxins, animal escape, personnel injury or illness, missing infectious material or toxins, unauthorized entry into the containment zone, power failure, fire, explosion, flood, or other crisis situations (e.g., earthquake, hurricane). Incidents include accidents and near misses.
Infectious material	Any isolate of a pathogen or any biological material that contains human or animal pathogens and, therefore, poses a risk to human or animal health.
Inventory	A list of (biological) assets associated with a containment zone identifying pathogens, toxins, and other infectious material in storage both inside and outside of the containment zone.
Mitigation measure	Measure that is implemented to prevent, detect, respond to, and recover from an event.
Pathogen	A microorganism, nucleic acid, or protein capable of causing disease or infection in humans or animals. Examples of human pathogens are listed in Schedules 2 to 4 and in Part 2 of Schedule 5 of the *Human Pathogens and Toxins Act*, but these are not exhaustive lists. Examples of animal pathogens can be found through the Automated Import Reference System on the Canadian Food Inspect ion Agency website.
Release	The discharge of infectious material or toxins from a containment system.
Residual risk	The risk remaining after the implementation of mitigation measures.
Risk	The probability of an undesirable event occurring (e.g., accident, incident, breach of containment) and the consequences of that event.
Risk group (RG)	The classification of biological material based on its inherent characteristics, including pathogenicity, virulence, risk of spread, and availability of effective prophylactic or therapeutic treatments, that describes the risk to the health of individuals and the public as well as the health of animals and the animal population.
Risk tolerance	The level of risk that an organization is willing to accept.
Security sensitive biological agents (SSBAs)	The subset of human pathogens and toxins that have been determined to pose an increased biosecurity risk due to their potential for use as a biological weapon. SSBAs are identified as prescribed human pathogens and toxins by Section 10 of the Human Pathogens and Toxins Regulations. This means all Risk Group 3 and Risk Group 4 human pathogens that are in the List of Human and Animal Pathogens for Export Control, published by the Australia Group, as amended from time to time, with the exception of Duvenhage virus, Rabies virus and all other members of the Lyssavirus genus, Vesicular stomatitis virus, and Lymphocytic Choriomeningitis Virus; as well as all toxins listed in Schedule 1 of the Human Pathogens and Toxins Act that are listed on the List of Human and Animal Pathogens for Export Control when in a quantity greater than that specified in Section 10(2) of the Human Pathogens and Toxins Regulations.

Senior management	The ultimate authority responsible for delegating appropriate biosafety authority. Senior management is responsible for ensuring that adequate resources are available to support the biosafety program, to meet legal requirements, and that biosafety and biosecurity concerns are appropriately prioritized and addressed.
Threat	An event or act, deliberate or accidental that could cause injury to people, information, assets, or services.
(Microbial) Toxin	A poisonous substance that is produced or derived from a microorganism and can lead to adverse health effects in humans or animals. Human toxins are listed in Schedule 1 and Part 1 of Schedule 5 of the *Human Pathogens and Toxins Act*.
Vulnerability (plural: vulnerabilities)	A weakness in a facility's physical security barriers, operational practices (e.g., biosecurity training), personnel security, transport security, information security, or program management.

CHAPTER 11

REFERENCES

CHAPTER 11 - REFERENCES

Defence Research and Development Canada. (2017). *The Chemical, Biological, Radiological/Nuclear Explosive (CBRNE) Consolidated Risk Assessment (CRA) Rating Tool Guide.* Ottawa, ON, Canada: Government of Canada. Retrieved 05/30, 2017 from http://cradpdf.drdc-rddc.gc.ca/PDFS/unc262/p805090_A1b.pdf

Government of Canada. (2016). *Canadian Biosafety Handbook* (2nd ed.). Ottawa, ON, Canada: Government of Canada. Available from https://www.canada.ca/en/public-health/services/canadian-biosafety-standards-guidelines/handbook-second-edition.html

Government of Canada. (2015). *Canadian Biosafety Standard* (2nd ed.). Ottawa, ON, Canada: Government of Canada. Available from https://www.canada.ca/en/public-health/services/canadian-biosafety-standards-guidelines/second-edition.html

Government of Canada. (2016). *Canadian Biosafety Guideline: Developing a Comprehensive Biosecurity Plan.* Ottawa, ON: Government of Canada. Available from https://www.canada.ca/en/public-health/services/canadian-biosafety-standards-guidelines/guidance/developing-comprehensive-biosecurity-plan-overview.html

Government of Canada, Communications Security Establishment, Royal Canadian Mounted Police. (2007). *Harmonized Threat and Risk Assessment Methodology, Version 1.0.* Ottawa, ON, Canada: Government of Canada. Retrieved 05/30, 2017 from https://www.cse-cst.gc.ca/en/publication/tra-1

Government of Canada. (2015). *Plan for Administrative Oversight for Pathogens and Toxins in a Research Setting - Required Elements and Guidance.* Ottawa, ON, Canada. Retrieved 05/30, 2017 from http://www.phac-aspc.gc.ca/lab-bio/licensing-licences/admin_oversight-surveillance_admin-eng.php

Government of Canada, Treasury Board of Canada Secretariat. (2012). *Policy on Government Security*. Retrieved 05.30, 2017 from https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578

Health of Animals Act (S.C. 1990, c. 21). (2017).

Health of Animals Regulations (C.R.C., c. 296). (2017).

Human Pathogens and Toxins Act (S.C. 2009, c. 24). (2015)

Human Pathogens and Toxins Regulations (SOR/2015-44). (2015).

ISO 31000:2009, Risk Management – Principles and Guidelines. (2009). Geneva, Switzerland: International Organization for Standardization.

Public Safety Canada. (2012). *All Hazards Risk Assessment: Methodology Guidelines, 2012-2013*. Ottawa, ON, Canada: Government of Canada. Retrieved 05/30, 2017 from https://www.publicsafety.gc.ca/cnt/mrgnc-mngmnt/mrgnc-prprdnss/ll-hzrds-rsk-ssssmnt-en.aspx

Public Safety Canada. (2017). *An Emergency Management Framework for Canada, Third Edition*. Ottawa, ON, Canada: Government of Canada. Retrieved 06/02 from https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2017-mrgnc-mngmnt-frmwrk/index-en.aspx

Public Safety Canada. (2013). *Building Resilience Against Terrorism: Canada's Counter-terrorism Strategy*. Ottawa, ON, Canada: Government of Canada. Retrieved 06/02 from https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/rslnc-gnst-trrrsm/index-en.aspx

Public Safety Canada. (2015). *Countering the Proliferation of Chemical, Biological, Radiological and Nuclear Weapons*. Ottawa, ON, Canada: Government of Canada. Retrieved 06/02 from https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cntr-trrrsm/cntr-prlfrtn/index-en.aspx

Salerno, R. M., & Gaudioso, J. (2007). *Laboratory Biosecurity Handbook*. Boca Raton, FL, USA: CRC Press.

United States Centers for Disease Control and Prevention, Division of Select Agents and Toxins & United States Animal and Plant Health Inspection Service, Agriculture Select Agent Program. (2013). *Security Guidance for Select Agent or Toxin Facilities (2nd Revision*). Retrieved 2017/02 from https://stacks.cdc.gov/view/cdc/22411

United States Congressional Research Service. (2007). *The Department of Homeland Security Risk Assessment Methodology: Evolution, Issues, and Options for Congress*. Retrieved 05/30, 2017 from https://fas.org/sgp/crs/homesec/RL33858.pdf

APPENDIX A

RESOURCES

APPENDIX A - RESOURCES

The following links, which were accurate at the time of publication, are external to the PHAC. The PHAC makes no guarantee that they remain active or that the content is up to date and accurate.

FEDERAL GOVERNMENT RESOURCES	
Canadian Security Intelligence Service (CSIS) www.csis.gc.ca	CSIS is responsible for investigating activities suspected of constituting threats to the security of Canada and to report these to the Government of Canada. CSIS publishes unclassified information products related to national security and intelligence issues, including: annual reports, world watch expert notes, occasional papers on priority issues, national and global security trends, outlooks, and potential risks and threats. Threat and analytical publications: www.csis.gc.ca/pblctns/index-en.php
Royal Canadian Mounted Police (RCMP) www.rcmp-grc.gc.ca	The RCMP is the Canadian national police service, which provides total federal policing services to all Canadians and policing services under contract to provinces, territories, municipalities, and aboriginal communities. Terrorism and Violent Extremism Awareness Guide: www.grc.gc.ca/qc/pub/sn-ns/sn-ns-eng.htm Suspicious Incident Reporting System (SIR): www.rcmp-grc.gc.ca/en/suspicious-incident-reporting-sir Extremist and Activist Groups: www.grc.gc.ca/qc/pub/sn-ns/ge-eg-eng.htm
Public Safety Canada (PS) www.publicsafety.gc.ca	Public Safety Canada is responsible for coordination across all federal departments and agencies that are responsible for national security and the safety of Canadians. The Canadian Disaster Database contains detailed disaster information on more than 1000 natural, technological and conflict events (domestic and international) that have happened since 1900 at home and abroad. www.publicsafety.gc.ca/cnt/rsrcs/cndn-dsstr-dtbs/index-eng.aspx Canadian Critical Infrastructure Information Gateway (CI Gateway) is a password protected workspace for public and private critical infrastructure stakeholders, and contains national security and emergency management products developed by federal organizations. cigateway.ps.gc.ca Counter proliferation of chemical, biological, radiological, and nuclear weapons: www.publicsafety.gc.ca/cnt/ntnl-scrt/cntr-trrrsm/cntr-prlfrtn/index-en.aspx Listed terrorist entities: www.publicsafety.gc.ca/cnt/ntnl-scrt/cntr-trrrsm/lstd-ntts/crrnt-lstd-ntts-eng.aspx Canadian Cyber Incident Response Centre (CCIRC), housed within Public Safety Canada, publishes cyber threat bulletins, and alerts, and produces quarterly summaries of cyber events that have affected Canadian business and critical infrastructure. www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/ccirc-ccric-eng.aspx

	Government Operations Centre (GOC), housed within Public Safety Canada, provides all-hazards integrated federal emergency response to events, including national-level situational awareness, warning products, risk assessments, national emergency management response policies and exercises. Unclassified products which are available to public and private partners are posted to the CI Gateway. www.publicsafety.gc.ca/cnt/mrgnc-mngmnt/rspndng-mrgnc-vnts/gvrnmnt-prtns-cntr-en.aspx
Communications Security Establishment of Canada (CSE) www.cse-cst.gc.ca	CSE is responsible for advice and guidance related to signals intelligence and cyber security. Top 10 IT Security Actions: www.cse-cst.gc.ca/en/node/1297/html/25231
Global Affairs Canada (GAC) www.international.gc.ca	GAC produces special reports on infectious diseases, travel advisories, and import and export controls. A Guide to Canada's Export Controls: www.international.gc.ca/controls-controles/about-a_propos/expor/guide.aspx?lang=eng
Public Health Agency of Canada (PHAC)	National authority on biosafety and biosecurity for human pathogens and toxins and a subset of terrestrial animal pathogens. Laboratory Biosafety and Biosecurity information and guidelines: www.canada.ca/en/services/health/biosafety-biosecurity.html
Canadian Food Inspection Agency (CFIA)	The CFIA establishes the biocontainment levels, procedures and protocols that are needed to work safely with animal and zoonotic pathogens, chemical hazards, and plant pests of quarantine significance and protects laboratory staff, the Canadian public, and the environment. Office of Biohazard Containment and Safety: www.inspection.gc.ca/animals/biohazard-containment-and-safety/eng/1300121579431/1315776600051
OTHER RESOURCES	
STRATFOR www.stratfor.com	Situational awareness reports, analysis and long-term threat environment forecasts and event analysis.
World Economic Forum www.weforum.org	Forward looking global risk forecasts https://www.weforum.org/reports
Crime Reports crimereports.com	Interactive maps of criminal incidents across participating jurisdictions, including Canada.
United States Centers for Disease Control and Prevention www.cdc.gov	*Historical trends related to bioterrorism: An Empirical Analysis*: wwwnc.cdc.gov/eid/article/5/4/pdfs/99-0406.pdf *Biosafety in Microbiological and Biomedical Laboratories (5th Ed.).* Washington, DC, USA: United States Government Printing Office. www.cdc.gov/biosafety/publications/bmbl5/index.htm
United States Department of Homeland Security, Federal Emergency Management Agency	*Risk Management Series: Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings.* www.fema.gov/es/media-library/assets/documents/2150

University of Bradford	*Preventing Biological Threats: What You Can Do*; and *Biological Security Education Handbook: The Power of Team-Based Learning* www.bradford.ac.uk/social-sciences/peace-studies/research/publications-and-projects/guide-to-biological-security-issues/
RELATED TOOLS AND RISK ASSESSMENT METHODOLOGIES	
Asset Value, Threat/Hazard, Vulnerability, and Risk www.fema.gov	A methodology for assessing risk of terrorism and natural hazards, as developed by the United States (U.S.) Federal Emergency Management Agency (FEMA). www.fema.gov/pdf/plan/prevent/rms/428/fema428_ch1.pdf
All-Hazards Risk Assessment (AHRA) Methodology www.publicsafety.gc.ca	The AHRA will help identify, analyze, and prioritize the full range of potential non-malicious and malicious threats. The process takes into account vulnerabilities associated with specific threats, identifies potential consequences should a threat be realized, and considers means to mitigate the risks. www.publicsafety.gc.ca/cnt/mrgnc-mngmnt/mrgnc-prprdnss/ll-hzrds-rsk-ssssmnt-en.aspx Public Safety Canada
Biorisk Assessment Models (BioRams) www.sandia.gov/	BioRams Software for assessing biosecurity events, with a focus on bioterrorism, developed by Sandia National Laboratories www.biosecurity.sandia.gov/BioRAM/ Sandia National Laboratories
Model for Risk and Vulnerability Analysis	brs.dk/eng/inspection/contingency_planning/rva/Pages/vulnerability_analysis_model.aspx Danish Emergency Management Agency
Harmonized Threat and Risk Assessment (TRA) Tool www.cse-cst.gc.ca www.rcmp-grc.gc.ca/en	The TRA is an unclassified publication, issued under the authority of the Chief, Communications Security Establishment (CSE) and Commissioner, Royal Canadian Mounted Police (RCMP). www.cse-cst.gc.ca/en/publication/tra-1 Communications Security Establishment of Canada; Royal Canadian Mounted Police
Regional Resilience Assessment Program (RRAP) publicsafety.gc.ca	Regional Resilience Assessment Program is a comprehensive risk assessment program for owners and operators of Canadian critical infrastructure. www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/crtcl-nfrstrtr-rrap-en.aspx.
International Standards Association (ISO) www.iso.org	*CAN/CSA-ISO 31000-10 (R2015) Risk Management – Principles and Techniques*
Canadian Standards Association (CSA) www.csagroup.org/	*CAN/CSA-ISO/IEC-CSA 31010-10 (R2015) Risk Management – Risk Assessment Techniques*
Hazard, Risk and Vulnerability Analysis (HRVA) Toolkit.	www2.gov.bc.ca/gov/content/safety/emergency-preparedness-response-recovery/local-emergency-programs/hazard-risk-and-vulnerability-analysis *Emergency Management British Columbia (EMBC). Government of British Columbia* www2.gov.bc.ca

APPENDIX B

BIOSECURITY ASSETS

APPENDIX B - BIOSECURITY ASSETS

The following is a sample list of assets that can be included in the biosecurity risk assessment.

Class	Category	Group	Component/Individual
Tangible	Biological Material	RG1	*Bacillus subtillis*
			Bacillus lichenformis
			Adeno-associated virus
		RG2	*Actinobacillus pleuropneumoniae*
			Hepatitis D virus
			Sporothrix schenkii
		RG3	*Mycobacterium tuberculosis*
			Penicillium marneffei
			Rabies virus
		RG4	Herpes B virus
			Hendra virus
			Lassa fever virus
		Toxin	Cholera
			Diphtheria
		SSBA	Shiga-like toxin (verotoxin)
			Bacillus anthracis
			Lassa virus
	Equipment	Biological Storage Equipment	Secure Freezer
			Lock Box
		Production Equipment	Fermenter
		Delivery System	Aerosolizer
		Physical Security	Intrusion detection system
			Electronic access control system
			Glass break sensors
			Closed circuit television
			Audible alarms
			Locks
			Shredders
			Fire alarms/detectors
	Software	Security	Alarms
			Intrusion detection system server
			Electronic access control system servers

	Information Technology (IT)	Hardware	Computer and peripherals
			Network access point
			Network printer
			External electronic storage drive
			Network storage
			Cloud storage
	Animal	Primate Colony	
		Mouse Colony	
Intangible	Information	Inventory	Pathogen and toxin
			Access authorizations and logs
			Building and floor plans (engineering plans)
			Database management system
		Proprietary Scientific Information	Processes
			Techniques
			Gene sequence
		Security	Biosecurity risk assessment
			Biosecurity plan
			Standard operating procedures
	Perception/Reputation	Employee Morale	
		Employee Confidence	
		Public Confidence	
		Competitive Advantage	

People	Personnel	Scientist	Professor
			Associate professor
		Student	Undergraduate
			Graduate
			Post-doctorate
		Administrative Support	Executive assistant
		Executive	Director
			Director general
			Dean
		Manager/Supervisor	Production
			Project
		Information Technology (IT) Personnel	Application and hardware support
			IT security specialist
		Safety and Security	Security officer
			Biological safety officer
	Contractor	Maintenance Personnel	Maintenance supervisor
			Maintenance personnel
		Facilities Personnel	Facilities manager
			Facilities personnel
		Security	Security guard/ commissionaire

APPENDIX C

BIOSECURITY EVENTS

APPENDIX C - BIOSECURITY EVENTS

The following is a sample list of biosecurity events that can be included in the biosecurity risk assessment.

Class	Category	Group	Event
Human Induced	Deliberate	Misuse	
		Unauthorized Release	Poisoning
			Disease/infection
		Diversion	In-transit
			Supply-chain hacking
		Extortion	Cyberextortion
			Ransom
			Kidnapping
			Reward
		Subversion	Lobbying
			Propaganda
			Political
		Sabotage	Destruction
			Vandalism
			Malware
			Denial of service
			Arson
			Supply-chain (e.g., equipment, services)
		Explosive	Bomb
		Espionage	Industrial (e.g., wiretapping, break-enter, coercion, sophisticated hacking, eavesdropping)
			State-sponsored (e.g., wiretapping, break-enter, coercion, sophisticated hacking, eavesdropping)
		Terrorism	Domestic
			International
		Criminal	Theft
	Accidental	Loss	

Appendix D

ADVERSARIES

APPENDIX D - ADVERSARIES

The following is a sample list of adversaries that can be included in the biosecurity risk assessment.

Adversary Class	Adversary Category	Adversary Group	Adversary
Insider	Personnel	Scientist	Professor
			Associate professor
		Student	Undergraduate
			Graduate
			Post-doctorate
		Administration	Executive assistant
		Analyst	Program analyst
		Executive	Director
			Director general
			Dean
		IT	Application and hardware support
			IT security specialist
		Office Staff	
		Safety and Security	Chief security officer
			Biological safety officer
	Contractor	Maintenance Personnel	
		Facilities Personnel	
		Security Guard / Commissionaire	

Outsider	Terrorist	International	
		Domestic	
		Radicalized Individual	
	State-Sponsored	Hacker	Elite hacker
			Amateur hacker
		Intelligence Service	
		Military	
		Department/Agency/Ministry	
		State Owned Enterprise	
	Non-State Sponsored	Organization	Competitor
		Activist and Militant Group	Animal
			Environmental
			Ecological
			Hackers
			Anarchist
			Hyper-nationalist
			Anti-globalization
	Lone Actor		
	Visitor	Canadian Citizen	
		Foreign National	
	Criminal	Crime Syndicate	
		Lone Actor	

APPENDIX E

BIOSECURITY MITIGATION MEASURES

APPENDIX E - BIOSECURITY MITIGATION MEASURES

The following is a sample list of biosecurity mitigation measures that can be included in the biosecurity risk assessment.

Class	Category	Group	Component
Physical Security	Security Barriers	Doors	Metal clad
			Hollow core
			Glass
			Aluminum
			Steel
			Solid core timber
		Windows	Glazed
			Tempered
			Sheet
			Bar guard
			Blast resistant
	Access Controls	Locks	Mechanical keys
			Electronic access control system (electronic keycard)
			Scrambled keypad
			Remote opening
			Biometrics
			Cipher key
			Keypad
			Master key lock series
			Padlock
			Latch bolts
			Deadbolts

	Monitoring and Surveillance	Closed Circuit Television	Camera (HD, night vision, 360)
			Camera coverage (blind spots, overlap)
			Storage of recorded media (short-term, long-term)
		Tamper Evident Technology	Tags
			Seals
			Labels
		Intrusion Detection	Infrared motion detection
			Motion detection
			Contact switches
			Acoustic motion
			Acoustic
			Glass break sensor (GBS)
			Software
			Sensor coverage (blind spots, overlap)
Information Security	Training and Awareness	Training	IT policies
			Removable storage media policy
Personnel Security	Standard Operating Procedures	Monitoring and Surveillance	Visual recognition
			CCTV monitoring
		Patrols	Security guards
		Protection	Executive
Security Program	Security Policies	Personnel Suitability and Reliability	Human Pathogen and Toxin Act Security Clearance
			Ongoing personnel reliability assessment program
			Criminal records history
			Proof of education
			Reference checks
			Credit checks
			Drug testing
		Storage of Material	Clear desk policy
			Closed office policy
			Document classification (e.g., proprietary, confidential, restricted)
			Inventory control (long-term storage)
		Information Dissemination	Policy on electronic recording devices (mobile phones, media players), lock-boxes in security zones

		Security During Movement and Transportation	Regulated material
	Access Controls	Visitor Control Procedures	Sign-in/sign-out (business hours)
			Sign-in/sign-out (after-business hours)
			ID verification
			Visitor escort (accompaniment and supervision)
			Visitor identification cards
		Personnel Control Procedures	Anti-tailgating policy
		Identification of Personnel	Access removal policy (ID cards, keys)
			ID cards
		Key Duplication Policy	
		Access Control System Records	Electronic access control system records of denied and granted access
	Incident and Emergency Response	Incident Investigation/Response Procedure	Release
			Equipment and intangible assets
		Incident Reporting	Suspicious behaviour (work during off-hours, unjustified requests for information, willful non-compliance, changes in behaviour)
			Incident report form or SOP
		Incident Response	Inventory discrepancy (pathogen or toxin)
			Equipment failure
			Lost or stolen ID card
			Lost or stolen laptop
			Removal of unauthorized individual
	Training and Awareness	Awareness	Insider threat training
			Handling of sensitive information
			IT security policies
			Security awareness
			Transfer of tangible and intangible assets
			Need to know
		Training Security Procedures	Suspicious individuals
			Suspicious package
			Electronic recording devices