Laboratory biosecurity guidance

World Health Organization

Laboratory biosecurity guidance

World Health Organization

Laboratory biosecurity guidance

This publication is the update of the document published in 2006 entitled *"Biorisk management: laboratory biosecurity guidance"*.

ISBN 978-92-4-009511-3 (electronic version)
ISBN 978-92-4-009512-0 (print version)

Suggested citation. Laboratory biosecurity guidance. Geneva: World Health Organization; 2024. Licence: CC BY-NC-SA 3.0 IGO.

Cataloguing-in-Publication (CIP) data. CIP data are available at https://iris.who.int/.

Contents

Foreword vi

Acknowledgements vii

Abbreviations and acronyms xii

Glossary of terms xiii

1 Introduction 1
- 1.1 Intended scope and target audience 2
- 1.2 How to use the laboratory biosecurity guidance 3

2 High-consequence research and gain-of-function experiments 4

3 Emerging technologies and potential threats 6
- 3.1 Genetic engineering 6
  - 3.1.1 Genome editing 6
  - 3.1.2 Gene drives 7
  - 3.1.3 Epigenetic manipulation 7
- 3.2 Synthetic biology 8
- 3.3 Artificial intelligence technology 8
- 3.4 Do-it-yourself biology 9
- 3.5 Misinformation and disinformation 10
- 3.6 Publication of high-consequence research 10

4 Biosafety/biosecurity programme management 12
- 4.1 Institutional biosafety/biosecurity policy 12
- 4.2 Institutional biosafety committee 13
  - 4.2.1 Roles and responsibilities of the institutional biosafety committee 14
  - 4.2.2 Institutional biosafety activities 15
- 4.3 Biosafety officer 16
  - 4.3.1 Role and core competencies 17
  - 4.3.2 Responsibilities and activities 18

5 Biosecurity risk assessment 19
5.1 Introduction 19
5.2 Strategies to lower risks inherent in work with biosecurity-relevant material 20
5.3 Types of laboratory biosecurity incidents 21
5.3.1 Incidents directly involving biological agents 21
5.3.2 Physical security incidents 21
5.3.3 Personnel-related biosecurity incidents 21
5.3.4 Incidents related to information security and cybersecurity 21
5.3.5 Deliberate events 22
5.3.6 Facilitating situations 22
5.4 Selecting the biosecurity risk assessment team 22
5.5 Risk assessment framework 22
5.6 Biosecurity risk assessment steps 23

6 Biosecurity risk control measures 25
6.1 Personnel reliability, screening, recruitment, competence and training 25
6.1.1 Personnel reliability and biosecurity culture 25
6.1.2 Personnel screening, recruitment, monitoring, support and protection 27
6.1.3 Personnel competence and training 29
6.2 Physical security 30
6.2.1 Facility security and access regulation 30
6.3 Inventory control and laboratory equipment 32
6.3.1 Laboratory inventory 32
6.3.2 National inventory 33
6.4 Destruction, decontamination and waste management 34
6.4.1 High-consequence material 34
6.4.2 Laboratory equipment, devices, information and software 34
6.5 Information security and cybersecurity 35
6.6 Emergency/incident prevention and preparedness 38
6.6.1 Reporting, investigation and corrective actions 39
6.6.2 Emergency destruction of high-consequence material 39

7 Transfer and transport of high-consequence material 41
7.1 International agreements 41
7.2 National legislation for the transport of high-consequence material 41
7.3 Biosecurity for the transfer and transport of high-consequence material 42
7.3.1 Fundamentals 42
7.3.2 Requirements 42
7.3.3 Personnel 44
7.3.4 Material transfer agreements 44
7.3.5 Transfer and transport of equipment with biosecurity relevance 45

8 National and international legislation and regulation 46
8.1 Best practices in national legislation and regulation on biological risks 46
8.1.1 Hybrid approach to regulate high-consequence material 47
8.1.2 Risk assessment 48
8.1.3 Gain-of-function experiments and high-consequence research 49
8.1.4 Possession, creation and sharing of high-consequence material 50
8.1.5 National inventory of high-consequence material and biosecurity-relevant equipment 51
8.2 International framework for biological risk legislation 52
8.2.1 United nations Secretary-General's Mechanism for Investigation of Alleged Use of Chemical and Biological Weapons 52
8.2.2 Biological Weapons Convention 52
8.2.3 International health regulations (2005) 53
8.2.4 Cartagena Protocol on Biosafety 54
8.2.5 Multilateral export control regimes 54
8.2.6 Guidance documents 55

9 References 56

10 Further information 59

Annex 1. Biosecurity risk assessment template 60

Annex 2. Biosecurity emergency response templates 78

Annex 3. Examples of national biosecurity laws, regulations, guidelines and policies 83

References – Annex 3 87

Foreword

Biomedical research and diagnostic tools play a crucial role in improving human health and combating infectious diseases. However, the foundation for these advancements lies in the handling and storage of infectious pathogens within laboratory settings. The intrinsic risks of working with biological agents are not only of a biosafety nature, such as exposure or unintentional release, but also of biosecurity, which includes the theft, misuse, or intended release of biological material.

Furthermore, the COVID-19 pandemic provided a meaningful opportunity to review the safety and security of laboratory practices ranging from day-to-day diagnostic testing to high-consequence research work, as well as the effectiveness of national oversight mechanisms. The World Health Organization (WHO) is committed to preventing epidemics and pandemics by ensuring the safe and secure handling of biological material in laboratories. To address this, the WHO published the fourth edition of the Laboratory Biosafety Manual in 2020, which takes a risk- and evidence-based approach to biosafety of laboratory work with biological agents. Complementary, the Laboratory biosecurity guidance has been revised to enhance the protection of laboratory operations against biosecurity threats. Both documents aim to enhance the biological risk management and prevent biosafety and biosecurity incidents.

To develop the Laboratory biosecurity guidance, the WHO engaged international experts to address biosecurity needs at the laboratory, institutional, and national levels. The WHO Technical Advisory Group on Biosafety (TAG-B) played a significant role in providing input and insights to create comprehensive guidelines that enable institutions to effectively manage biosecurity risks in collaboration with national regulatory bodies. A focus of the Laboratory biosecurity guidance is the biosecurity risk assessment, the strengthening of the review function of the institutional biosafety committees and the proposal of a two-tier system of national oversight.

Acknowledgements

Principal coordinator

Dr Kazunobu Kojima, Epidemic and Pandemic Preparedness and Prevention, World Health Organization, Switzerland

Editorial committee

- Professor Stuart Blacksell, University of Oxford/Mahidol-Oxford Tropical Medicine Research Unit, Thailand
- Dr Samuel Edwin, Division of Select Agents and Toxins, Center for Preparedness and Response at the Centers for Disease Control and Prevention (CDC), United States of America
- Dr Katharina Summermatter, Biosafety Center and Managing Director of the Biosafety Level 3 Laboratory, Institute for Infectious Diseases at the University of Bern, Switzerland

Contributors - Technical advisory group on Biosafety (TAG-B) members

- Dr Salama Al Muhairi, Research and Development of HazMat Department, National Emergency Crisis and Disasters Management Authority (NCEMA), United Arab Emirates
- Professor Atanu Basu, National Institute of Virology, India
- Dr Sergey Aleksandrovich Bodnev, Epidemiology of Highly Dangerous Virus Infections laboratory and Reference Center for orthopoxviruses and other dangerous infection diseases at the Federal Budgetary Research Institution - State Research Center of Virology and Biotechnology (VECTOR), Rospotrebnadzor, Russian Federation
- Dr Aissam Hachid, Medicine Faculty and Arboviruses and emerging viruses laboratory at the Human Virology Department, Pasteur Institute of Algeria, Algeria
- Professor Aamer Ikram, National Institutes of Health, Pakistan
- Ms Morgan Kafenzakis, Centre for Biosecurity, Public Health Agency of Canada (PHAC), Canada
- Mr David Lam, Singapore General Hospital, Singapore
- Mr Zibusiso Masuku, National Institute for Communicable Diseases (NICD) of the National Health Laboratory Service (NHLS), South Africa
- Ms Leonora Nusblat, Biocontainment Unit at the National Administration of Laboratories and Institutes of Health, Argentina
- Dr Indrawati Sendow, Research Center for Veterinary Science, Research Organization for Health, National Research and Innovation Agency (BRIN), Indonesia
- Dr Jane Shallcross, Novel and Dangerous Pathogens Training Team, United Kingdom Health Security Agency (UKHSA), United Kingdom of Great Britain and Northern Ireland
- Ms Sacha Wallace-Sankarsingh, Caribbean Public Health Agency (CARPHA); PAHO/AMRO; International Federation of Biosafety Associations (IFBA), Trinidad and Tobago
- Professor Guizhen Wu,National Institute for Viral Disease Control and prevention (IVDC), China CDC, China

Contributors – Individuals*

- Dr Leon Caly, Victorian Infectious Diseases Reference Laboratory, Australia
- Dr Isabelle Daoust-Maleval, European Commission, Belgium
- Ms Sandhya Dhawan, Epidemic and Pandemic Preparedness and Prevention, World Health Organization, Switzerland
- Dr Julian Druce, Victorian Infectious Diseases Reference Laboratory, Australia
- Dr Mirko Himmel, University of Hamburg, Germany
- Dr Markus Huber, Epidemic and Pandemic Preparedness and Prevention, World Health Organization, Switzerland
- Dr Catherine Makison Booth, Health and Security Executive, United Kingdom of Great Britain and Northern Ireland
- Mr Rohit Malpani, Research for Health, World Health Organization, Switzerland
- Dr Christina Scheel, US Department of Labor, United States of America
- Mr Dallas Wilson, Victorian Infectious Diseases Reference Laboratory, Australia

*Individual subject matter experts supplementing the expertise of the TAG-B members

Project management

Ms Rica Zinsky, Epidemic and Pandemic Preparedness and Prevention, World Health Organization, Switzerland

Reviewers - Individuals

- Mr Mahdi Aljewary, Iraqi National Monitoring Agency, Iraq
- Dr Iris E. Andernach, Federal Ministry of Health, Germany
- Professor Paul Arbon, James Cook University, Australia
- Mr Allan Bennett, United Kingdom Health Security Agency (UKHSA), United Kingdom of Great Britain and Northern Ireland
- Dr Åsa Szekely Björndal, Public Health Agency of Sweden (PHAS), Sweden
- Dr Rik Bleijs, National Institute for Public Health and the Environment (RIVM), Netherlands (Kingdom of the)
- Dr Susann Boggs, Sandia National Laboratories, United States of America
- Professor Malcolm Dando, University of Bradford, United Kingdom of Great Britain and Northern Ireland
- Ms Leanne DeWinter, International Experts Group of Biosafety and Biosecurity Regulators (IEGBBR), Canada
- Professor Ricardo Dias, University of Lisbon / Portuguese Ministry for Science & Technology, Portugal
- David Elliott, United Kingdom International Biosecurity Programme, United Kingdom of Great Britain and Northern Ireland
- Leila Lany M. Florento, Biorisk Association of the Philippines, Philippines
- Dr David Franz, United States of America
- Professor Joachim Frey (retired), University of Bern, Switzerland

- Ms Line Gemynthe Gylling, Centre for Biosecurity and Bioprepardness, Denmark
- Mrs Ghada Ghaleb Almadaw (retired), Ministry of Health, Iraq
- Dr Vips Halkjaer-Knudsen, Vipsit LLC ApS, Denmark
- Dr Keith Hamilton, World Organisation of Animal Health, France
- Dr David Harper, Chatham House, United Kingdom of Great Britain and Northern Ireland
- Dr Sara Holditch, United States of America
- Dr David Holmes, Centers for Disease Control and Prevention, United States of America
- Dr Thomas V. Inglesby, John-Hopkins University, United States of America
- Mr Geofrey Jagero, United States Centres for Disease Control and Prevention (US CDC) Kenya, Kenya
- Dr Tessy Joseph, National University of Singapore, Singapore
- Dr Andreas Kurth, Robert-Koch-Institute, Germany
- Mr Hermann Alex Lampalzer, Biological Weapons Convention, Switzerland
- Dr James Le Duc, United States of America
- Dr Filippa Lentzos, King's College London, United Kingdom of Great Britain and Northern Ireland
- Dr Poh Lian Lim, Tan Tock Seng Hospital and National Centre for Infectious Diseases, Singapore
- Dr Talkmore Maruta, Africa Centre for Disease Control and Prevention, Ethiopia
- Dr Jusaku Minari, Kyoto University, Japan
- Ms Abigail Padua Miranda, Griffith University, Australia
- Dr Gerald W. Parker, Texas A&M University, United States of America
- Dr Sabai Phyu, EU CBRN CoE Centres of Excellence Initiative – Southeast Asia Region/ Laboratory Biorisk Consultancy & Training (LBCT) Pte. Ltd, Singapore
- Dr Mark Rayfield, Centers for Disease Control and Prevention, United States of America
- Dr Saskia Rutjes, National Institute for Public Health and the Environment (RIVM), Netherlands (Kingdom of the)
- Dr Sjors Schulpen, National Institute for Public Health and the Environment (RIVM), Netherlands (Kingdom of the)
- Dr Nariyoshi Shinomiya, National Defense Medical College, Japan
- Mr Edson Michael M. Simon, Biorisk Association of the Philippines, Philippines
- Professor Jozef Suvada, St. Elizabeth University of Public Health and Social Work & McMaster University & Scranton University & Ministry of Health, Slovakia
- Dr Gladys Gek Yen Tan, DSO National Laboratories, Singapore
- Ms Iris Vennis, National Institute for Public Health and the Environment (RIVM), Netherlands (Kingdom of the)
- Dr Rodel Vitor, De La Salle University, Philippines
- Ms Laurie Wallis, Sandia National Laboratories, United States of America
- Professor Leifan Wang, Tianjin University, China
- Dr Go Yoshizawa, Kwansei University, Japan
- Professor Weiwen Zhang, Tianjin University, China

Reviewers - Organizational

- American Biological Safety Association (ABSA) International
- Canadian Government (Food Inspection Agency, Global Affairs Canada, Public Health Agency of Canada)
- Mexican Biosafety Society
- United States of America Government

Reviewers - WHO Headquarters

- Dr Soatiana Rajatonirina, Science Division, World Health Organization, Switzerland
- Dr Anna Laura Ross, Science Division, World Health Organization, Switzerland
- Dr Nahoko Shindo, Epidemic and Pandemic Preparedness and Prevention, World Health Organization, Switzerland
- Dr Harpal Singh, Polio Eradication, World Health Organization, Switzerland
- Ms Lisa Stevens, Country Readiness Strengthening, World Health Organization, France
- Dr Emmanuelle Tuerlings, Science Division, World Health Organization, Switzerland
- Dr Maria Van Kerkhove, Epidemic and Pandemic Preparedness and Prevention, World Health Organization, Switzerland

Reviewers - WHO Regional offices

- Mr Mustafa Aboualy, Infectious Hazard Prevention and Preparedness, World Health Organization, Egypt
- Dr Amal Barakat, Infectious Hazard Prevention and Preparedness, World Health Organization, Egypt
- Ms Victoria Katawara, Country Health Emergency Preparedness and IHR, World Health Organization, Philippines
- Dr Luke Meredith, Infectious Hazard Prevention and Preparedness, World Health Organization, Egypt

Financial support

Development and publication of this document have been made possible with financial support from the Defense Threat Reduction Agency, US Department of Defense.

Conflict of interest

Declaration of interest forms were collected from external contributors and reviewers and evaluated by WHO. None of the reported interests were found to be relevant.

Abbreviations and acronyms

ADR	Agreement concerning the international carriage of dangerous goods by road
AI	Artificial Intelligence
AMRO	Regional Office for the Americas
BMBL	Biosafety in microbiological and biomedical laboratories
BRIN	National Research and Innovation Agency
CDC	Centers for Disease Control and Prevention
DIY	do-it-yourself
DNA	Deoxyribonucleic acid
EU CBRN CoE	European Union Centres of Excellence on Chemical, Biological, Radiological and Nuclear Risk Mitigation
EU	European Union
IBC	Institutional Biosafety Committee
IEGBBR	International Experts Group of Biosafety and Biosecurity Regulators
IFBA	International Federation of Biosafety Associations
IHR	International health regulations
IMDG	International maritime dangerous goods
IVDC	National Institute for Viral Disease Control and prevention
JEE	Joint External Evaluations
LBM4	Laboratory Biosafety Manual, fourth edition
NCEMA	National Emergency Crisis and Disasters Management Authority
NHLS	National Health Laboratory Service
NICD	National Institute for Communicable Diseases
PAHO	Pan American Health Organization
PHAC	Public Health Agency of Canada
PHAS	Public Health Agency of Sweden
RID	Regulations concerning the international carriage of dangerous goods by rail
RIVM	National Institute for Public Health and the Environment
RNA	Ribonucleic acid
SPAR	State Party self-assessment report
TAG-B	Technical advisory group on Biosafety
UKHSA	United Kingdom Health Security Agency
UN	United Nations
VECTOR	State Research Center of Virology and Biotechnology
WHO	World Health Organization
Wi-Fi	Wireless Fidelity

Glossary of terms

Accident. An inadvertent, unintentional or negligence-caused occurrence that results in: actual harm, such as infection, illness, injury in humans, animals or plants, or contamination of the environment; unauthorized access; loss; theft; or misuse, diversion, or release or weaponization of the biosecurity-relevant material, technology or data.

Accountability. An obligation to accept responsibility and to account for high-consequence material and other biosecurity-relevant material, by formally associating specified materials and the responsibility for their control and tracing with specific individuals.

Bioethics. The study of the ethical and moral implications of biological discoveries, biomedical advances, and their applications in diagnostics, research and work with high-consequence material. Bioethics also includes the consequences of unsafe research for the individual researcher, the institution and society. In this document, bioethics is one component that contributes to successful biosafety/biosecurity programme management.

Biological agent. A microorganism, virus, biological toxin, particle or otherwise infectious material, either naturally occurring or genetically modified, which may potentially cause infection, allergy, toxicity or otherwise create a hazard to humans, animals or plants.

Biological risk management. An umbrella term that describes biosafety and laboratory biosecurity measures.

Biosafety. Containment principles, technologies and practices that are implemented to prevent unintentional exposure to biological agents or their inadvertent release.

Biosafety/biosecurity programme management. The development, implementation and oversight of biosafety and biosecurity at the institutional level using a variety of information that includes institutional policies, guidance documents for practices and procedures, planning documents (training, recruitment, emergency/incident response) and record-keeping (personnel, inventories, incident management).

Biosafety officer. An individual designated with the responsibility and authority to oversee facility or institutional biosafety (and possibly biosecurity) programmes. This person may also be considered as a biosecurity officer, biosafety/biosecurity professional, biosafety/biosecurity adviser, biosafety/biosecurity manager, biosafety/biosecurity coordinator or biosafety/biosecurity management adviser.

Biosecurity. Policies, principles, technologies and practices implemented for the protection and control of and accountability for biological material, technology and information or the equipment, methods, skills and data related to their handling. Biosecurity aims to prevent intentional or accidental unauthorized access to, and loss, theft, misuse, diversion or release or even weaponization of such commodities.

Biosecurity-relevant material. Any material, technology and information that could be of importance if an incident were to occur such as unauthorized access, loss, theft, misuse, diversion or release, but that does not have characteristics of high-consequence material. Such material includes biological agents, nucleic acids, synthetically derived biohazardous material, laboratory devices, software and data.

Biosecurity risk assessment. A systematic process of gathering information, evaluating the consequences of a biosecurity risk and vulnerabilities, and determining/defining the appropriate risk control measures to reduce the risk to an acceptable level.

Certification. A third-party testimony based on a structured assessment and formal documentation confirming that a facility, system, person or piece of equipment conforms to specified requirements, for example, to a certain standard.

Code of conduct (code of practice, code of ethics). Non-legislated guidelines for behavioural and practical standards that are voluntarily accepted or a legally binding part of a biosafety/biosecurity programme and followed as best practice.

Consequence (of a laboratory biosecurity incident). The outcome of a biosecurity incident of varying severity, occurring in the laboratory or in a location associated with the laboratory. Consequences may include exposure to or release of a biological agent, a deliberate or accidental loss of biosecurity-relevant material, their theft, the mixing of a non-pathogenic (or less pathogenic) biological agent with a high-consequence pathogen or unauthorized access to a laboratory and/or information.

Containment. The combination of physical design parameters and operational practices that protect personnel, the immediate work environment and the community from exposure to biological agents. The term biocontainment is also used in this context.

Cybersecurity. Prevention of damage to, and protection and restoration of computers, electronic communications systems, electronic communications services, wire communications and electronic communications, including information contained therein, to ensure their availability, integrity, authentication and confidentiality. In the laboratory context, cyber access to laboratory equipment and building systems is the critical and aimed at protecting against attacks.

Decontamination. Reduction of viable biological agents or other hazardous materials on a surface or object(s) to a predefined level that is no longer of biosecurity risk by chemical and/or physical means.

Disinformation. Wrong or misleading information shared in full knowledge that it is false, often with malicious intent.

Emergency response plan. An outline of a structured and approved set of behaviours, processes and procedures to be followed when handling sudden or unexpected situations, including exposure to or release of biological agents, or a biosecurity incident. An emergency/incident response aims to prevent and/or minimize injuries or infections or limit their consequences, reduce damage to equipment or the environment, and accelerate the resumption of normal operations.

Engineering controls. Risk control measures built into the design of laboratory structures, systems, and equipment to contain hazards. Biological safety cabinets and isolators are forms of engineering controls to minimize the risk of exposure to and/or unintended release of biological agents.

Epigenetics. Study of inheritable but reversible phenotypic characteristics not coded by nucleic acids but affecting gene expression. These characteristics could be acquired by interaction with the environment.

Exposure. An event during which an individual comes in contact with, or is in close proximity to, biological agents with the potential for infection or harm. Routes of exposure can include inhalation, ingestion, percutaneous injury and absorption and are usually dependent on the characteristics of the biological agent. However, some routes of exposure of certain pathogens are specific to the laboratory environment and are not commonly seen in the general community.

Gain-of-function. Modification of biological agents that results in a new or enhanced property or function not previously associated with the biological agent. The term is often used to label research on pathogenic properties that result in enhanced pathogenesis or other characteristics that could cause harm besides an intended benefit. In this guidance, gain-of-function is exclusively used with this second meaning.

Genetic engineering. Modification of nucleic acids with molecular methods and technology that results in changes in the characteristics of an organism.

Genetically modified organisms. Organisms whose genetic material has been modified by using genetic engineering techniques such as recombinant nucleic acid technology or genome editing. The term generally does not cover organisms whose genetic composition has been altered by conventional crossbreeding or so-called mutagenesis breeding, as these methods predate the discovery of recombinant nucleic acid techniques (1973). The related term for microorganisms is genetically modified microorganisms.

Hazard. An object or situation that can potentially cause adverse effects when an organism, system or (sub) population is exposed to it. In the case of laboratory biosafety, the hazard is defined as biological agents that can potentially cause adverse effects to humans, animals, and the wider community and environment. A hazard does not become a risk until the likelihood and consequences of that hazard causing harm are considered. The term biohazard is specifically used in the laboratory biosecurity context.

High-consequence material. A biological agent, biological material or technology and the information about it that is capable of causing, direct or indirect, disease or other significant harmful effects in humans, animals, plants and/or the environment.

High-consequence research. Research with intended benefits that uses or creates material, technology or information that could cause significant harmful effects in humans or their social systems (such as their economy), animals, plants and/or the environment.

Incident. An action or occurrence that has the potential to, or results in, the exposure of laboratory personnel to biological agents and/or their deliberate or accidental release that may or may not lead to actual harm.

Infectious substances. Any material, solid or liquid, that contains biological agents capable of causing infection in humans and/or animals. Infectious substances can include patient specimens, biological cultures, medical or clinical waste and/or biological products such as vaccines. The term is used in the context of transportation in this guidance.

Initial risk. Risk associated with laboratory activities or procedures conducted without risk control measures.

Institutional biosafety committee. An institutional working group created to act as an independent review group for biosafety and laboratory biosecurity issues in laboratory activities, such as research or diagnostics. The membership of the committee should reflect the different occupational areas of the institution as well as its scientific expertise.

Laboratory. A facility within which biological agents, their components or their derivatives are collected, handled and/or stored. Biological laboratories include clinical research laboratories, hospital laboratories, diagnostic facilities, regional and national reference centres, public health laboratories, research centres (for example, academic, pharmaceutical, environmental), mobile laboratories, regulatory laboratories and production facilities (for example, manufacturers of vaccines, pharmaceuticals, large-scale biologicals) for human, veterinary and agricultural purposes. Related sites such as repositories, waste-handling areas and places where environmental samples are taken are seen as locations where biosafety and biosecurity policies are applied and are included in the broader sense of this definition.

Likelihood (of a laboratory biosecurity incident). The possibility that a defined actor would select a given tactic and successfully exploit a particular vulnerability to acquire or affect a specific target.

Mobile laboratories. So-called on-wheels infrastructures consisting of laboratories inside trucks, vans, train or other modular equipment in place in a vehicle. These include those that are dropped at or shipped to laboratory/research locations and used as a temporary laboratory facility or integrated with an existing laboratory facility.

Misuse. The illegitimate or inappropriate use of material, technology and/or information that deviates from established protocols, agreements, treaties, codes of conduct and conventions.

Misinformation. Wrong and misleading information shared without malice.

Near miss. An incident as defined above that does not have adverse consequences but needs to be reported so systems can be improved to prevent future incidents.

Pathogen. A biological agent capable of causing disease in humans, animals or plants.

Regulator. An independent governmental authority that assesses and controls the handling of certain materials, activities and information on a national level.

Residual risk. Risk that remains after carefully selected risk control measures have been applied. If residual risk is not acceptable, it may be necessary to apply additional risk control measures or stop the laboratory activity.

Risk. A combination of the likelihood of an incident occurring and the severity of its consequences (harm) if that incident were to occur.

Risk assessment. A systematic process of gathering information and evaluating the likelihood and consequences of exposure to or release of workplace hazard(s) and determining the appropriate risk control measures to reduce the risk to an acceptable risk.

Risk communication. An interactive, proactive and systematic process to exchange information and opinion on risk(s) that inclusively engages all relevant personnel of various categories and community leaders and officials where appropriate. Risk communication, as a risk control measure, is an integral and ongoing part of the risk assessment. It intents a clear understanding of the risk assessment process and outcomes that aims to properly implement risk control measures. Decisions on risk communication, including what, whom and how, should be part of an overall risk communication strategy.

Risk control measure. Use of a combination of tools, which include communication, assessment, training, and physical and operational controls, to reduce the risk of an incident/event to an acceptable level. The risk assessment cycle will determine the strategy that should be used to control the risks and the specific types of risk control measures required to reduce risk.

Standard operating procedures. A set of well-documented and validated stepwise instructions outlining how to perform laboratory practices and procedures in a safe, timely and reliable manner, in line with institutional policies, best practice and applicable national or international policies and/or regulations.

Threat. A malicious intention and ability to cause an adverse event, including injury, disruption, damage, theft, diversion, misuse, unauthorized access, intentional release of materials or information, or sabotage.

Toxin: Poisonous substance produced by living cells or organisms.

Virulence. The level or intensity of pathogenicity of an organism as indicated by mortality from the associated disease and/or ability to invade and cause disease.

Workflow (laboratory workflow). A stepwise series of processes and activities in the laboratory by which an experiment, assay, method or other project passes from initiation to completion. Process planning and administration enables the development of algorithms and/or standard operating procedures that define sequential steps in each process. Workflow process algorithms may include descriptions of facilities, services, systems and space required for each step to optimize understanding of and communication between staff for optimal safety and productivity. Workflow algorithms as standard operating procedures can be further detailed to include the flow of personnel, specimens, materials and waste.

Zoonotic diseases (zoonoses). Infectious diseases naturally transmitted from animals to humans and vice versa.

1 Introduction

Biosecurity risk control measures aim to safeguard biological material from laboratory biosecurity incidents, such as theft, misuse, or unauthorized access. Biosecurity incidents could lead to serious or even catastrophic outcomes if high-consequence material is involved, resulting in economic repercussions and public concerns and fears. The first edition of the laboratory biosecurity guidance was published in 2006 *(1)*. This current revision aims to provide guidance on ways to work safely and securely with high-consequence material and biosecurity-relevant material and how to build capacity at institutional and national levels to address biological risks to ensure that scientific progress continues while minimizing risks to the community and environment.

The WHO Laboratory biosecurity guidance has been developed by the WHO Laboratory Biosafety and Biosecurity Programme in consultation with the WHO technical advisory group on biosafety (TAG-B). The members of the TAG-B joined working groups to develop the sections of the Laboratory biosecurity guidance and other subject-matter experts were consulted to supplement the expertise of the advisory group members. The draft has undergone two reviews and all steps of the progress of the revision have been guided and monitored by the TAG-B. This edition of the Laboratory biosecurity guidance is a complete revision of the 1st edition published in 2006. The major advancements are the adjustment to the LBM4 with applying the risk- and evidence-based approach also to laboratory biosecurity, the emphasis of understanding laboratory biosecurity and biosafety as a continuum, the inclusion of new developments in science and technology and to address laboratory biosecurity on all three levels: the laboratory, the institution and the national regulatory body.

Laboratory biosecurity is inseparable from biosafety (Fig. 1.1), and both areas complement each other to ensure safe and secure laboratory operations. The term biological risk management describes the continuum of biosafety and biosecurity at the institutional and national levels. In 2020, the World Health Organization (WHO) published the fourth edition of the *Laboratory biosafety manual, fourth edition (2)* (LBM4) which promotes a risk- and evidence-based approach to biosafety. The risk assessment framework in the laboratory biosafety manual enables institutions to develop and implement locally relevant, effective and sustainable (fundable over a longer period) risk control measures to manage biosafety risks associated with working with biological agents. For the development of this laboratory biosecurity guidance, the risk- and evidence-based approach is applied to high-consequence research and other activities with biosecurity-relevant material, technology and/or information. The guidance addresses risks from the point-of-view of laboratory biosecurity at both the institutional and national level.

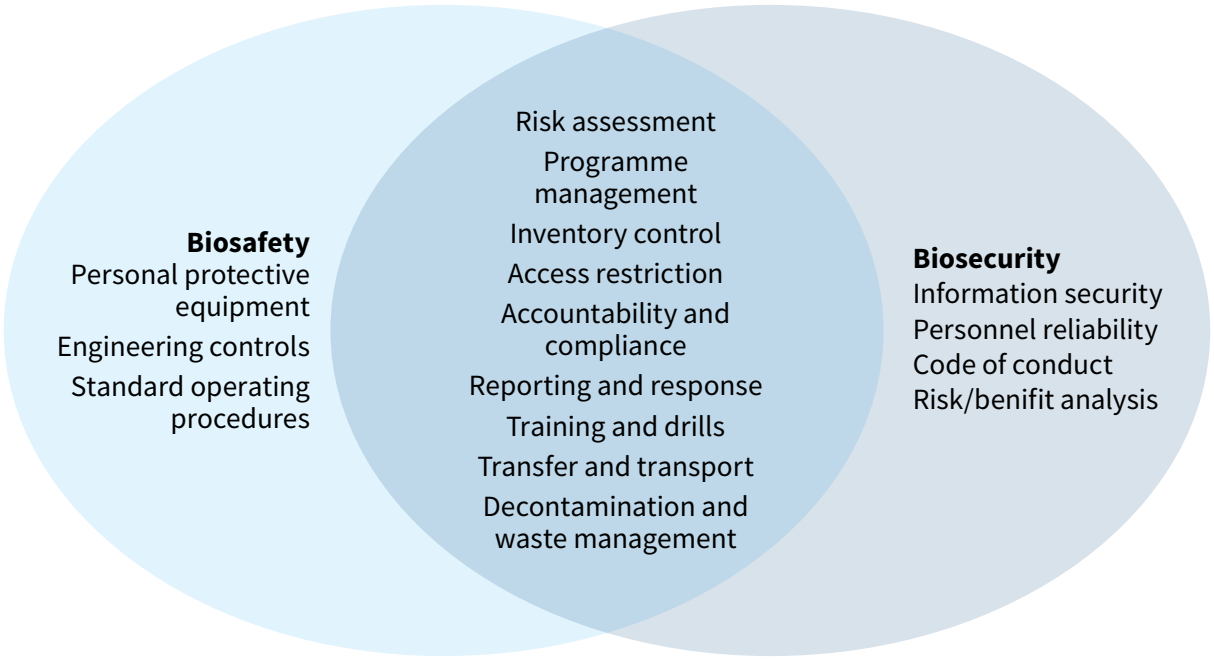

Fig. 1.1. Spectrum of biological risk management: examples of overlapping elements of biosafety and laboratory biosecurity

In the monitoring and evaluation framework of the *International health regulations* (2005 (IHR (2005)) *(3)*, biosafety and biosecurity are assessed in the IHR State Party self-assessment report *(4)* (SPAR) and they are one of the 19 technical areas evaluated in the joint external evaluations *(5)* (JEE). In 2021, at the 74th World Health Assembly, the importance of laboratory biosecurity was recognized by Member States in the session on enhancement of laboratory biosafety *(6)*, and this mandate is the basis of the revision of the laboratory biosecurity guidance.

It is also important to consider that findings in life science research projects intended for the benefit of humans and the environment sometimes have the potential for malicious use and can be misused to cause harm to society and the environment *(7)*. Furthermore, rapid technological developments and advances in methods manipulating biological material in the past decade have redefined the biological threat landscapes. These biosecurity-relevant issues are considered in this laboratory biosecurity guidance.

1.1 Intended scope and target audience

This publication provides guidance to institutions, national regulatory bodies and other involved stakeholders (for example, funding organizations and scientific publishers) to establish a framework to identify, manage and oversee biosecurity risks in laboratory activities and the life cycle of high-consequence material and other biosecurity-relevant material in different institutions.

The guidance covers high-consequence research and work with high-consequence material and other biosecurity-relevant material. The principles described in this document could be applied to various laboratory settings, material, technology and information of different biosecurity relevance.

The term biosecurity in the laboratory context used in this guidance largely relates to laboratory activities. It should not be confused with the term biosecurity that is used in environmental and agricultural sciences to refer to managing risks associated with the introduction and release of modified living organisms and their products, and the introduction and management of invasive alien species.

This guidance follows the principles of the risk- and evidence-based approach for biosafety introduced in WHO's *Laboratory biosafety manual, fourth edition* for laboratory biosecurity *(2)*. A biosecurity risk assessment template with an embedded high-consequence decision tree was developed to identify biosecurity risks, high-consequence research and high-consequence material and implementing biosecurity risk control measures to address the identified biosecurity risks.

The document provides tools and guidance to manage laboratory biosecurity risks and outlines best practices at the three vertical levels: laboratory, institution and national regulatory levels. It also outlines best practices at the horizontal level: for example, sample collection, transport, processing, storage and, if necessary, destruction in places such as diagnostic laboratories (fixed or mobile), research institutions, manufacturers and pharmaceutical companies, among others.

One key to capacity and capability building of biological risk management is to establish and/or strengthen the institutional biosafety committees (IBC) function for review of high-consequence research and work with high-consequence material. To promote this aspect, the guidance describes a two-tier system engaging both IBCs in the first instance and national regulatory bodies in the second. To this end, the document describes in detail the roles and responsibilities of both parties, with IBCs providing oversight of high-consequence work within their institution, and then passing feedback to national regulatory bodies who maintain inventory lists and storage of restricted material.

1.2 How to use the laboratory biosecurity guidance

This laboratory biosecurity guidance provides tools for the institutional management, scientists, laboratory personnel, biosafety officers, members of IBCs, the national regulatory body and others to identify and control biosecurity risks. With the biosecurity risk assessment templates, this guidance provides the user with a systematic method to address their specific biosecurity risks and implement sustainable and locally relevant risk control measures. Furthermore, the guidance presents risk control measures and best practices for the work with high-consequence material and other biological material of biosecurity relevance in different areas, for example: personnel reliability, screening, recruitment, competence and training; physical security; inventory control and laboratory equipment; destruction, decontamination of biosecurity relevant material and waste management; cybersecurity and information security; and emergency/incident prevention and preparedness.

2 High-consequence research and gain-of-function experiments

To emphasise the importance of addressing biosafety and biosecurity risks of research with biological material that could have severe or even catastrophic consequences to life, the laboratory biosecurity guidance uses the term high-consequence research to describe these experiments. Other terminology is used such as dual-use research of concern, dual-use, or research of concern. High-consequence research is at risk of potential malicious use of biological agents as well as unintentional exposure and/or release of such agents, despite its intended benefits. Hence it is of both biosafety and laboratory biosecurity concern. While some work can be clearly classified as high-consequence research, the aims and effects of other research may not be so obvious.

High-consequence material has the ability to cause harmful effects with severe or even catastrophic consequences. Similar terms for such material in this context are pathogens, valuable biological material, high-impact material and information, potential pandemic pathogens, enhanced potential pandemic pathogens, biological materials with epidemic or pandemic potential, or biological agents.

This document includes a decision matrix with a series of questions that guide the categorization of different types of high-consequence research and materials which can be used by researchers, national authorities and other relevant persons/bodies. The following criteria have been developed to identify high-consequence research and high-consequence material in the biosecurity risk assessment.

Does the laboratory work plan to use or produce biological material known to have one of the following characteristics?

- Ability to interfere with, bypass or reduce the effectiveness of therapeutic or prophylactic treatment or vaccination
- Enhanced virulence, communicability, transmissibility or potential to cause death
- Increased pathogenicity
- Altered host range and tropism, including potential inadvertent selection by serial passage on cells of human or other new host species
- Ability to evade detection methods and diagnostics
- Potential use as a severely harmful biological material or even a biological weapon
- Production of toxins, increased toxin production, or enhanced toxicity of an existing toxin
- Increased stability and resistance to decontamination
- Altered absorption, toxicokinetic or host susceptibility
- Ability to bypass natural immunity
- Enhanced capacity for spreading or easy dissemination

Can research knowledge (data, methodology, results), technologies and intermediate or final products (such as toxins or nucleic acid) be misused to cause harm?

- Yes/no

If released, could the biological agent, material or research information pose a risk to any of the following?

- Humans
- Environment
- Animals, plants, fungi, microorganisms
- National public health and safety

If the answer to any of the above questions is yes, the laboratory work could be regarded as high-consequence research or work with high-consequence material and would need a biosafety and biosecurity risk assessment (see section 5 Biosecurity risk assessment).

Laboratories engaged in high-consequence research are required to have a comprehensive training programme to increase awareness among principal investigators, scientists and laboratory personnel of biosecurity risks and associated responsibilities. More information on this aspect can be found in in subsection 6.1.3 Personnel competence and training. Furthermore, a strong biosafety/biosecurity programme involving the IBC needs to be in place to ensure risk assessments are conducted and suitable risk control measures are implemented. More information on this aspect can be found in section 4 Biosafety/biosecurity programme management.

When planning high-consequence research projects, several factors should be considered before work starts. The decision to conduct high-consequence research is based on balancing the expected benefits for society and the potential consequences of a biosafety or biosecurity incident. For an informed decision, biosafety and biosecurity risk assessments (see Annex 1. Biosecurity risk assessment template) and risk/benefit analysis should be performed.

Subsection 8.1, Best practices in national legislation and regulation on biological risks, describes a two-tier system for the national regulation of high-consequence research.

3 Emerging technologies and potential threats

The development of openly accessible methods and technologies across many scientific disciplines has the potential to contribute substantially to the advancement of sciences, particularly the understanding of the molecular biology of infectious agents. These same advances, however, also provide the opportunity for adaptation for more nefarious purposes, which could pose significant risks to the public. Thus, high-consequence research needs to be evaluated so that suitable frameworks can be developed to minimize the risks without compromising the benefits to the population *(8)*. Such evaluation is now more feasible and accessible because of emerging technologies.

The advances in sciences and diagnostic methods enable less well equipped laboratories to perform laboratory work with biosecurity relevance. This section discusses established molecular methods and emerging disciplines, such as gene editing, synthetic biology, gene drives, artificial intelligence (AI), epigenetic modifications and do-it-yourself (DIY) laboratories, to enable the reader to carry out risk assessments and address risks that may occur during research projects with the methods and technologies described or conducted in non-laboratory environments.

Regardless of their level of involvement in the biosecurity risk management process, all personnel (for example, scientists, principal investigators, students and technical assistants) engaged in research, diagnostics or other work where a biosecurity risk is identified should familiarize themselves with the principles of this guidance. They should be able to identify and evaluate the biosafety and biosecurity risks as they apply to their work, which could be high-consequence research or work with high-consequence material or with otherwise biosecurity-relevant material.

3.1 Genetic engineering

Genetic engineering describes laboratory technologies for modifying the composition of an organism's DNA, such as cutting out a specific genetic sequence to modify, remove, and/or insert genetic information or switch off genes.

The purchase and use of genetic engineering kits, consumables, platforms and methods is largely unregulated, but the creation of genetically modified organisms is restricted in several countries. The easy application of the methods not only facilitates this work in standard laboratories but also in DIY laboratories (see subsection 3.4 Do-it-yourself biology). In these latter laboratories, there is the possibility that genetic engineering experiments are carried out without ethical and biosecurity institutional supervision and may pose a biosafety risk because they are carried out with low-quality equipment and without academically and technically qualified personnel.

3.1.1 Genome editing

Genome editing is largely facilitated by the availability of molecular methods that are easily applicable even in basic laboratories. Unfortunately, this straightforward technique could be

misused for harmful purposes and it lowers technical barriers to the development of high-consequence biological material. Therefore, the experiments conducted and the method and equipment used have biosecurity relevance due to their universal usability *(8)*.

Genome editing has enormous potential for improving human health, agriculture and the environment, but it can also cause substantial and irreversible harms. Such harms might include the uncontrolled diffusion of genome edited material in the environment, off-target effects from genome editing, or the disruption to ecologies with genetically altered organisms. Harms may also arise by deliberate use of these techniques to target humans and/or the environment. Such intentional misuse of genome editing techniques requires two circumstances: the availability of techniques and know-how that could be exploited for irresponsible or nefarious purposes (so-called information hazard), and the ability to use such knowledge and tools to generate and disseminate harmful engineered organisms *(9)*.

Furthermore, the technical requirements for genome editing methods can be very basic and inexpensive, enabling not only conventional laboratories, but also DIY laboratories, to use these methods easily.

3.1.2 Gene drives

Gene drives are naturally occurring, or genetically engineered constructs used to maintain specific genetic information in an organism through multiple generations. Gene drives are an artificial selection factor that could lead to the extinction of specific genetic information *(10, 11)*. While the application of gene drives (naturally occurring or genetically engineered) holds promise for genetic solutions for diseases or control of populations of invasive species, it also has the potential for harm if misused, including potential extinction of certain genetic material or species.

3.1.3 Epigenetic manipulation

Manipulation of the epigenome involves chemical modifications of nucleic acids and histone proteins that do not alter the genetic code itself but change genetic expression patterns that could be passed down to the next generation. Currently, limited data are available on the influence of epigenetic factors on replication processes in pathogens and the formation of the host immune response. The most studied non-genetic mechanisms are described for regulation of carcinogenesis. Epigenetic regulation is central to producing different and heritable gene expression patterns. Five well-studied mechanisms of epigenetic regulation have been described: DNA methylation; nucleosome positioning; diverse histone variants; post-translational modifications; and regulatory RNAs.

Some epigenetic modifications are also capable of repressing pathogen gene expression. However, a wide variety of DNA and RNA viruses frequently exploit these mechanisms to regulate their life cycles. For example, DNA viruses often use such cellular mechanisms to regulate their biological activities because they rely on epigenetic or similar processes to make different viral genome states coexist in the cell during infection.

Furthermore, these epigenetic regulators are known to affect viral pathogenesis by expanding tissue tropism, evading the cell's innate immune response and establishing a persistent latent infection, or driving host–cell carcinogenesis. Additionally, triggers of epigenetic modification may potentially be used to alter pathogenicity and/or a host's immune response, pathogenesis, clinical manifestation of disease *(12, 13)*.

3.2 Synthetic biology

Synthetic biology is a discipline for redesigning biological systems (from molecular structures to whole organisms) for advantageous purposes by engineering them to have new abilities or properties. Synthetic biology has great potential for beneficial and useful applications but products could also be misused to harm humans or the environment. It is a new interdisciplinary field involving biotechnology, chemistry and engineering, among others. Bioengineering, as part of synthetic biology, is the design of entirely new signalling pathways, including multiple genes and regulatory elements. Bioengineering aims to design new biological systems using abstract and simplified metabolic and regulatory modules and other standardized components that can be combined freely into new pathways or organisms *(14)*.

Governance systems must balance mitigating the risk of misuse with supporting opportunities for innovation and development *(9)*, which could include commercial screening of potentially high-consequence gene sequences. The rapid development of synthetic biology and its promise have raised a number of ethical concerns, which the community of experts in the field has been addressing *(15)*.

Artificial DNA synthesis based on DNA polymerase is not a new technology, the novelty is the ability to synthesize DNA fragments with longer nucleic acid chains in a shorter turnaround time for the synthesis process. In the past, devices with this technology were not part of molecular laboratories. However, the further development of such devices with desktop applications and lower costs allows more institutions and DIY laboratories to acquire a commercially available DNA synthesizer with little to no regulation.

Furthermore, these technologies allow shorter DNA fragments to be combined into genomes that can then be transfected in host cells and expressed in the modified organism. This raises the concern that even basic models of a DNA synthesizer could be misused to create high-consequence pathogens.

The Australia Group Common Control List *(16)* has influence in certain countries on the legislation on biological and chemical weapons, their precursors and the components that could be used to manufacture them. Certain pathogens are listed for which the synthesis of DNA is restricted *(17)*. This listing is an exception as regulation of the synthesis of genes, genomes and DNA sequences is lacking. However, several international and national efforts are underway to improve guidance and oversight in nucleic acid synthesis, such as commercial screening of potentially high-consequence gene sequences.

3.3 Artificial intelligence technology

Information technology systems that integrate artificial intelligence (AI) are already used in biosecurity-relevant applications and programmes. They will soon play a wider and more critical role in all sectors.

While AI could support biosecurity-relevant laboratory operations in the broadest sense, for example, research, diagnostic and closed circuit television surveillance, there might be AI technologies that can enable or facilitate the creation of high-consequence material, technology or information that have the potential to be misused as harmful biological material or even a biological weapon or otherwise pose risks to humans or the environment. For example, first, while AI can help identify and develop investigational compounds de novo through protein language models, the same AI technologies could also be used to develop new toxic compounds

(18, 19). Second, the emergence of large language models and multimodal models, which can be used to summarize relevant information or generate responses to queries, has proven too often to confabulate responses and even generate non-existent references, which could mislead or misdirect an individual who chooses to rely upon such information (see subsection 3.5 Misinformation and disinformation). Third, the results of AI applications might have an intrinsic potential to generate false positives or encode certain biases based on the dataset on which the AI technology was trained, or the results may not reflect or be not sufficiently congruent with the data used to train the AI technology. Fourth, a more humanistic concern could be ethical standards that are not integrated into the design of the AI technology or that may not be implemented in its deployment and use. Finally, national or international policies or regulations intended for AI technologies may not be amended or adopted with sufficient speed and flexibility to address the newest developments in AI applications.

WHO considers that AI technology can help improve the health of populations *(20)*. The group identified 15 new and emerging technologies and scientific advances that may have a significant impact on global health in the next 2 decades. Among these technologies is AI and machine learning applications. However, even when created with best intentions, AI-supported programmes have the potential to be misused. For example, there might be AI technologies, or uses of AI technologies, that enable or facilitate the creation of high-consequence material with the potential for misuse or that could pose a threat to society or the environment. AI could also facilitate de novo synthesis of dangerous viruses or new, more transmissible strains of viruses. Thus, AI models need to be built in ways that do not increase those risks.

3.4 Do-it-yourself biology

DIY biology is a global biotechnological movement in which amateurs, enthusiasts, students and trained scientists conduct biological studies outside scientific institutions. The term DIY biology is often used synonymously with garage biology, citizen science and biohacking, among others *(21)*, and the community follows hacker ethics, such as sharing, openness and world improvement.

DIY biology has been gaining popularity as it offers individuals the opportunity to pursue biology projects without needing to justify a monetary profit or particular advantage, is often driven by curiosity or personal interest, and has played a positive role in the development of biotechnological applications such as cheap and simple diagnostic tools *(22)*.

Despite its popularity and advantages, the nature of DIY biology makes it challenging to ensure biosafety and biosecurity practices are implemented. Moreover, members of the DIY biology community are not necessarily trained in biosafety or biosecurity, and they do not necessarily follow established and accepted standards for safe and secure laboratory work – for example, infrastructure of facilities, working practices, equipment, biosafety and biosecurity risk assessments, and risk control measures. Now, with the development of effective tools to manipulate nucleic acid easily, quickly and cheaply, work with high-consequence material could be done with basic laboratory equipment and could evade regulation as the experiments can be performed outside registered and regulated institutes.

Many established DIY communities, whether online or in person *(23)*, have enacted voluntary compliance with codes of ethics, self-identified laboratory registries and government regulations for laboratories working with pathogens. Regulatory bodies should provide programmes and initiatives to raise awareness about biosafety and biosecurity risks among the DIY community.

3.5 Misinformation and disinformation

Misinformation and disinformation could influence laboratory personnel and externals (for example, service provider, technicians or other people without authorized access to facilities), which may lead to biosecurity incidents. It is necessary to distinguish between disinformation and misinformation *(24)*. Misinformation is typically viewed as so-called accidental falsehoods, that is, wrong and misleading information shared without malice. On the other hand, disinformation is a so-called deliberate falsehood, that is, wrong or misleading information shared in full knowledge that it is false, and often with malicious intent. Misinformation and disinformation feed off each other to a certain extent: disinformation will be amplified and often snowball through misinformation. AI-generated information also needs to be considered as it could create misinformation.

Disinformation may mainly target laboratories holding high-consequence material and/or conducting high-consequence research. The media coverage of laboratory work with high-consequence material, and hence the impact it has on society, is influenced by the duality of the biological sector and the recollection of epidemics, for example, the medieval black plague. The depiction in the pop culture of uncontrollable epidemics with high morbidity and mortality maintains this damaging perception of such work. Disinformation can generate an epidemic of doubt and confusion and reveal and aggravate societies' and vulnerabilities.

Among the essential factors a biology laboratory to consider to ensure security of its activities are the human resources (for example, personnel), the high-consequence research itself, the methods used, the facility, and the equipment. The human factor can be the first to be destabilized by disinformation, which will potentially lead to a cascade of undesirable effects that may affect the rest of the laboratory.

Human vulnerability could in unintended consequences.

- Stressed laboratory personnel might be under psychological pressure to avoid any biosafety and biosecurity incident. In this context, disinformation campaigns will increase this psychological pressure substantially. These personnel may indeed be physically threatened, taken hostage, or even have their families threatened. This stress can obviously also lead to unintentional errors, directly impacting the biosafety and biosecurity of the whole laboratory.
- Disinformation campaigns could also affect people especially those who have pre-existing psychological disorders. If these people support a cause, disinformation could give them an additional justification and push them to act or accelerate their actions, whether against laboratory staff or directly against the laboratory itself.
- Disinformation could generate and/or amplify the probability of internal threats (for example, from dissatisfied employees, temporary employees, activist employees and student trainees) as well as external threats (for example, from activists or terroristic groups, service providers, suppliers, competitors, former employees, inspectors and auditors).

3.6 Publication of high-consequence research

Scientific publication of biosecurity-relevant information (such as, high-consequence research, nucleic acid sequences of high-consequence material or virulence factors) should be carefully considered. While publishing research results is valued and encouraged in the scientific

community, certain research results, methods, genetic information or programmes may be used for malicious purposes.

Policies that distinguish between information that should be published or partly published and information that should be omitted in an article (or other publication or communication) that is accessible to the public need to be established by the scientific community, such as, scientists, publishers and peer-reviewers, for example, based on WHO's guidance on this *(7, 25)* on an international level. On a national level such policies need to be implemented by the regulatory body for high-consequence research/material and by the IBC on an institutional level *(26)*. These efforts should include scientists, editors, reviewers of scientific journals, donors and regulatory bodies.

4 Biosafety/biosecurity programme management

This section describes the establishment and maintenance of an institutional biosecurity programme. Ideally, laboratory biosecurity will be incorporated into the existing biosafety programme management framework as detailed in the *Laboratory biosafety manual (2)* and the accompanying *Biosafety programme management* monograph *(27)*. The recommendations in this section can be used as a stand-alone guide for establishing and integrating biosecurity programme elements in the facility, institution or laboratory since biosecurity is often part of the overall institutional biosafety programme. Alternatively, biosecurity can be managed separately through a biosecurity policy or other biosecurity-relevant areas can be addressed in committees, such ethics or genetic engineering committees. This section focuses on biosecurity-relevant elements within the biosafety programme. In the regulation of high-consequence research or material in a country, the biosafety/biosecurity programme is an important component. As recommended in subsection 8.1 (Best practices in national legislation and regulation on biological risks), the IBCs are an essential part of the two-tier approach in the regulation of high-consequence research or material.

4.1 Institutional biosafety/biosecurity policy

The primary aim of a biosecurity programme is to prevent loss, theft and misuse of high-consequence material. This can be done by providing and implementing risk control measures that address the risks associated with conducting high-consequence research and working with high-consequence material, including other biosecurity-relevant material. The context of the use of high-consequence material within the institution should be clearly explained in the institution's' biosafety/biosecurity policy. This policy should also define the activities, responsibilities and competencies of the biosafety officer, the IBC and other personnel related to biosecurity. Communication strategies and, if applicable, the components of a code of conduct should also be defined in the policy.

As the main programme guidance document, the institutional policy for biosafety and biosecurity clearly states an institution's biosafety and biosecurity objectives, associated intentions and targets. It demonstrates the relevance of and commitment to biosafety and biosecurity within an institution. The scope of the policy depends on the size and complexity of the facility, the activities performed and the associated risks, for example, activities with high-consequence material.

In the policy, the communication of risks should be specified. The internal communication of risks might follow the recommendations given in the *Biosafety programme management monograph (27)*. In contrast, the strategy for the external communication of biosafety and biosecurity risks may be the responsibility of the senior management of the institution. The policy can also define the target audience, type and detail of information of the risk, frequency of updates and the form its publication may take.

4.2 Institutional biosafety committee

The IBC is commissioned to provide expert knowledge and consultation about biosafety and biosecurity risks and to recommend and implement risk control measures to lower these risks. The IBC is responsible for reviewing the biosafety and biosecurity aspect of projects that involve, but are not limited to, genetic engineering, pathogens, human materials and other potentially infectious material, as well as transgenic animals. The IBC provides recommendations for the communication to the community on matters pertaining to the control of biohazards associated with the use of biological agents and their vectors. The committee also need to consider the interests of the surrounding community with regard to public health and the protection of the environment. The IBC reviews and approves all research and instructional activities involving biohazardous material before the activity is started. The committee ensures that biological work under its responsibility is reviewed independently, and that appropriate controls, practices and procedures are in place for the work to be conducted safely and securely. As an independent committee, the IBC will be responsible for reviewing biosecurity risk assessments and research applications for potential high-consequence research and material, and reporting biosecurity breaches. As such, policies about conflict of interest are important to ensure the independence of IBC members.

Depending on the size of the institution and the kind of laboratory activities conducted, the roles and responsibilities for biosafety and biosecurity could be separated. In this case, in addition to a biosafety officer and an IBC, a biosecurity officer and an institutional biosecurity committee could be established. As biosafety and biosecurity risk control measures may overlap with each other (see Fig. 1.1), good communication and cooperation between the teams responsible for biosafety and biosecurity are necessary. This guidance uses the terms biosafety officer and IBC, even though the names, roles and responsibilities may vary between institutions.

Furthermore, the IBC may develop clear objectives, strategies and policies for lowering institutional biosafety and biosecurity risks. To achieve their objectives, the IBC will be mandated with the overall monitoring of the biosafety/biosecurity programme and advising and reporting to the senior management of the institution. All activities of the IBC should be documented.

The IBC should meet regularly (with the meetings documented), depending on the type of activities and the associated risks of high-consequence material and other biosecurity- and biosafety-relevant issues.

Membership of the committee should be through appointment by the top management. Members should serve a predefined term, for example, 2 years, depending on the availability of experts in an institution.

The exact functions and responsibilities of the IBC, its composition and its working methods, including reporting, are to be described by the IBC.

The IBC should include members with the collective technical and scientific expertise to review and evaluate all the matters referred for consideration, assessment and advice by the institution(s) for which it acts. Membership on the IBC should be proportionate to the institution´s size and the risks associated with the activities within the institution. Committee members should have expertise in relation to the work conducted in the institution, and cover the following areas (non-exhaustive list):

- biosafety and laboratory biosecurity (for example, the biosafety officer),
- microbiology (for example, bacteriology, virology, parasitology, mycology),

- veterinary practices and zoonoses,
- legal requirements, especially for high-consequence material,
- emerging technologies (for example, gain-of-function studies, gene drives),
- information technology, bioinformatics and cybersecurity,
- facility operation (for example, security, building, maintenance, engineering, waste streams),
- bioethics and social science (for example, inclusion of a representative of the institutional ethical committee), and
- epidemiology, infection prevention, occupational health and the environment.

Additional internal or external experts in other areas may be called in, either as observers in an advisory capacity or as permanent members, provided that a confidentiality agreement is in place. Especially in smaller institutions with unexpectedly identified high-consequence research, external experts could complement an IBC to ensure the committee meets the required biosafety and biosecurity needs of the institution.

4.2.1 Roles and responsibilities of the institutional biosafety committee

The IBC may assign roles and responsibilities in the terms of reference document to select members to help achieve its goals and objectives. IBC meetings should be managed so that information, including research protocols, incident reports and meeting minutes, is distributed and available to all members. The committee should be structured so that all members are informed of the agenda well in advance to provide them with the opportunity to prepare any reports or material needed. Activities and progress towards goals should also be tracked for review and improvements as required.

Typically, a chairperson, or chair, will be appointed or elected, for example, by a majority vote at the first meeting of the committee or by the senior management of an institution. This chair should be a senior person with skills to manage the tasks of the IBC and the ability to communicate, negotiate and resolve issues arising during meetings. Furthermore, the chair must be independent of the research being evaluated to avoid bias and conflict of interest. The chair is responsible for leading the meetings and setting goals together with all IBC members. The chair will also assign other committee roles, including the formation and leadership of subcommittees as needed, and ensure that the appointed individuals fulfil their roles in a timely and efficient manner. A vice-chair may be required to assist the chair and take on leadership duties in his/her absence. A new chair should be assigned annually or every 2 years to ensure continuity of operations and prevent leadership bias and burnout.

A secretary should be appointed to manage all administrative functions of the IBC. The secretary will prepare the meeting agenda with the chairperson and communicate the meeting arrangements to the IBC members. In addition, the secretary will take minutes of the meetings and ensure that these are prepared and delivered to members. The committee may seek the assistance of external advisers as and when required.

Meetings should occur regularly at specified intervals so that IBC members can commit to attending them well in advance. In practice, the IBC should meet once monthly initially, but the frequency may change based on the IBC's scope of duties and the size of the institution.

4.2.2 Institutional biosafety activities

The IBC uses the expert knowledge of its members to implement strategies, policies and guidelines that reduce institutional biosafety and biosecurity risks. These strategies, policies and guidelines must promote accepted best practice and adhere to national and international regulations to ensure institutional compliance.

The IBC oversees the identification of high-consequence research and/or other biosecurity risks. The IBC should be given review/oversight authority and, in collaboration with the principal investigator, approve or reject projects based on expected benefit versus the potential to cause harm.

The following are examples of IBC activities intended to fulfil its responsibilities.

- Ensure the implementation of national regulations, international biosafety and biosecurity standards and best practices, and keep informed of new technology developments. This responsibility also includes compliance with bioethical standards, undertaking of risk/benefit analyses and taking carefully weighted decisions on the suitability of studies with specific biosafety-related risk.
- Implement the policies and guidelines for institutional compliance with national and international legislation and advise institutional leadership on those requirements.
- Provide advice and facilitate training and capacity-building programmes on biosafety and biosecurity for personnel working with high-consequence material.
- Facilitate the development and periodic updating of institutional biosafety/biosecurity manuals and emergency response plans, including procedures for shipping and receipt of biological and infectious substances.
- Establish an institutional code of conduct, especially if high-consequence research is performed.
- Ensure operational security for the business processes of the IBC.
- Provide technical oversight of the institution's biosafety/biosecurity programme and reports to senior management, which includes:
    - assessing laboratory infrastructure against a predefined standard(s);
    - acting as custodian of evidence that the institution's laboratories are registered or accredited as required by applicable laws;
    - monitoring laboratory activities through audit reports and accident/incident reports relating to biosafety and biosecurity;
    - ensuring that national regulations are implemented/considered;
    - developing a strategy and system for governance of good biosafety and biosecurity practices as they relate to the institution's research and other laboratory-based projects;
    - ensuring that inventory control and documentation are in place, recorded and followed for receipt, storage, transfer, shipping and destruction of high-consequence pathogens and materials; and
    - using a holistic approach to biosafety and biosecurity and performing/overseeing an overarching risk assessment of high-consequence research and/or regularly reviewing all ongoing research projects with high-consequence material.
- Review protocols for proposed research and all high-consequence research products (manuscripts, white papers, grant applications) before publication to ensure the following.

- Investigators have used appropriate risk assessment and risk control strategies for biosafety and biosecurity risks, with additional risk control strategies and risk control measures being put in place as required.
- The principal investigator notifies the IBC if there are unexpected results from the high-consequence research.
- The rationale and/or hypotheses are provided for protocols that include genetic modifications and/or gene expression (genome editing, synthetic nucleic acid molecules, recombinant proteins) of biological agents.
- Proposed outcomes of the research are feasible and the benefits outweigh the remaining risks identified.
- Genetic modifications of pathogens are well described for all protocols and include nucleic acid sequence data (including primers), vectors and organisms that will be used in the research project.
- All high-consequence research information products (manuscripts, white papers, grant applications) are reviewed before publication.

- Advocate for laboratory biosafety and biosecurity within the institution to gain institutional and financial support for biosafety and biosecurity.

To provide the most current guidance and assistance to their institutions, IBCs must stay informed about changes in biosecurity policies and requirements. Changes may include new policies at the national and international level, changes in safety regulations at the local or national level, and changes in requirements and practices by regulatory or accrediting bodies. To prepare for such changes, the IBC should frequently communicate with the relevant bodies and share the information gathered with their institutional leaders, the IBC and relevant researchers. In this way, preparations can be made to provide personnel training for new procedures, update policy, guidance and/or procedure at the institution, and purchase necessary risk control measures.

Subsection 8.1 (Best practices in national legislation and regulation on biological risks) of this guidance document describes additional IBC activities and strategies where an IBC/regulatory body hybrid approach is used to oversee and regulate high-consequence research and material.

4.3 Biosafety officer

According to the *Laboratory biosafety manual* monograph on biosafety programme management *(27)*, "A biosafety officer should be appointed to provide advice and guidance to personnel and management on biological safety issues. The role and knowledge of the biosafety officer is key to developing, implementing, maintaining and continually improving a biosafety and biosecurity programme."

The responsibilities of the biosafety officer depend on several factors, for example, the size of the institution, volume and type of research performed at the institution, national legislation, and the presence and quantity of high-consequence pathogens. In many cases, the biosafety officer will also be responsible for the biosecurity programme. However, in institutions with more biosecurity-relevant elements, such as those conducting high-consequence research or working with high-consequence material, one or more designated employee may be responsible for biosecurity. In this case, the tasks, responsibilities and competencies must be defined.

The biosafety officer may work on the bench for a laboratory where their responsibilities may include quality control and overall laboratory management. Large institutions that work with high-consequence pathogens may have several tiers of biosafety programme management, each with greater authority and institutional oversight.

If the availability of experts allows, biosafety officers and others with authority over the biosafety/biosecurity programme management should report through a separate chain of authority from those of the laboratories they oversee to avoid bias and potential conflict of interest. Furthermore, the top management needs to provide adequate resources for the biosafety officer to implement a comprehensive biosafety/biosecurity management programme.

The biosafety officer is independent of those responsible for implementing biosafety and biosecurity measure or conducting activities within an institution. The biosafety officer should report directly to senior management and have the authority to prohibit work if deemed necessary. An institution should lay out the necessary conditions of the job of biosafety and biosecurity officer, including a job description outlining roles, responsibilities, competencies and decision-making power related to the function.

4.3.1 Role and core competencies

Depending on the laboratory or institutional activities, a biosafety officer should have an appropriate background and practical experience in applicable life sciences, biomedical science and/or biomedical engineering. In addition, persons with substantial practical experience, training and/or certification in biosafety and biosecurity and relevant security management disciplines from recognized institutions would be suitable candidates.

For example, in laboratories where work with high-consequence material or high-consequence research is conducted, the biosafety officer should have comprehensive theoretical and/or practical knowledge of: biosecurity aspects of this work and adapted to the needs of the institution; existing national legislation; laboratory methods, practices and procedures; and risk control measures.

Where possible, a biosafety officer will have completed training specific to biosafety and biosecurity practices and procedures, and should have demonstrated practical experience. Continuing education and maintenance of the core competencies for a biosafety officer are necessary for this role.

To successfully fulfil the role, the biosafety officer should demonstrate a high degree of discretion, tact, and team-building and communication skills to support the implementation of a sustainable culture of biosafety and biosecurity compatible with institutional needs and expectations.

4.3.2 Responsibilities and activities

The laboratory biosafety manual *(2)* and its accompanying monograph on biosafety programme management *(27)*, describe in further detail the actionable responsibilities of the biosafety officer, which may vary depending on the size and scope of research at the institution.

The biosafety officers may need to undertake the following activities to fulfil their responsibilities and duties in the biosecurity field.

- Participate as a member of the IBC.
- Raise awareness of biosecurity issues among the institution's personnel at all levels.
- Facilitate and support the principal investigator/scientist in performing biosecurity risk assessments.
- Review biosecurity risk assessments.
- Recommend biosecurity risk control measures informed by a risk assessment.
- Conduct biosecurity-specific consultations on technical and security procedures for working with biological agents at all stages of research (planning, implementation, close and/or routine intervals where applicable).
- Develop risk-control strategies, practices and procedures to eliminate or reduce the identified biosecurity risks in collaboration with relevant stakeholders.
- Monitor implementation of and adherence to approved facility-specific biosafety and biosecurity policies and procedures.
- Conduct internal audits and assessments to identify vulnerabilities.
- Promote and monitor the implementation of legislative/regulatory and non-legislative requirements and ethical best practices (for example, relevant codes of conduct), reporting back to the IBC.
- Develop, organize and deliver biosecurity training based on the risk assessment and identified user needs.
- Develop and maintain the institutional biosafety/biosecurity manual.
- Participate in the reporting, investigation and follow-up of biosecurity accidents, incidents, and near misses.
- Develop emergency plans and conduct exercises/drills on dealing with laboratory accidents and biosecurity incidents.
- Coordinate inspections with independent third-party assessors.
- Inform laboratory personnel and senior management of the relevant hazards, their likelihood of occurring, and their consequences.
- Ensure interaction and coordination with other areas relevant to safety or security, such as chemical safety.
- Report biosecurity-relevant findings, make improvements in biosecurity risk control measures and monitor progress of the implementation of risk control measures.
- Oversee infectious waste management.

5 Biosecurity risk assessment

5.1 Introduction

To prevent laboratory biosecurity incidents with high-consequence material and other biosecurity-relevant material, risk assessment needs to be done to guide the implementation of risk control measures.

A biosafety risk assessment framework was developed in the laboratory biosafety manual *(2)* and outlined in detail in the monograph on risk assessment *(28)*. The biosecurity risk assessment could follow the same systematic process of gathering information (identification of risks and vulnerabilities), evaluating the risks associated with the laboratory activity (pathogens, toxins, knowledge, information and personnel), developing a risk control strategy, implementing risk control measures, and reviewing risks and risk control measures. For biosecurity risk assessments, a thorough analysis of potential targets, threat perpetrators and their potential tactics, and related vulnerabilities that can be exploited are critical to selecting appropriate risk control measures. Other approaches for biosecurity risk assessment, besides the laboratory biosafety manual risk assessment framework *(2)*, exist and can also be used.

Biosecurity risks can be challenging to assess because many factors contribute to these risks including the intent of the individual(s). For example, the intention of an individual interested in obtaining laboratory materials is difficult to identify but it poses a biosecurity risk. Awareness training on insider threats can be developed and provided to all personnel to mitigate this biosecurity risk. In addition, the accidental release of material relevant to biosecurity is a biosecurity risk, but it is difficult to assess because it involves human factors. Therefore, it is important to define and establish a systematic and site-specific biosecurity risk assessment process within an institution, especially for work with high-consequence material. Furthermore, laboratory biosecurity aims to address laboratory risks and threats outside of accidental exposure or release. Biosecurity risk assessments, which are part of the institutional biosafety/biosecurity programme, are performed, documented and reviewed by laboratory personnel, the biosafety officer and/or the IBC.

For biosecurity risks, the likelihood component might be disregarded, so the consequences are mainly considered. This approach differs from the definition and application of risk used in the laboratory biosafety manual *(2)*. Another difference from a biosafety risk assessment is the range of biological material, technology and information relevant to biosecurity that needs to be considered. In addition to biological agents, which include high-consequence material and which are mainly considered here, other biological material, technology, information and personnel must be also considered.

Moreover, risk control measures for biosafety and biosecurity may overlap and/or interfere with one another. For example, for emergency response, when to prioritize site security over containment measures needs to be decided. Other examples of overlap and decisions that may have to be taken include:

- exchange of information related to high-consequence material or exchange of this material in the case of a disease outbreak so as to, for example, develop tests;

- publicly available information related to activities or facilities (public register of activities, accidents and incidents) or personnel involved in high-consequence research versus biosecurity control measures; and
- publication of lessons learnt from accidents and incidents which may be prohibited depending on the type of incident.

In such cases, risk-based priorities must be evaluated with considerations of alternatives, planned and coordinated. Identified high-consequence research requires the implementation of biosecurity risk control measures, but also an assessment or re-assessment of biosafety risks.

Biosecurity and biosafety risks should always be considered together. As such, another component of a biosecurity risk assessment is the recommendation to perform or review the research project or the diagnostic work with a biosafety risk assessment, especially if characteristics of high-consequence research or material were identified in the biosecurity risk assessment.

In this section, different components of the biosecurity risk assessment process are described.

5.2 Strategies to lower risks inherent in work with biosecurity-relevant material

When planning a research project, laboratory biosecurity risks can be reduced from the very outset, at the design of the research proposal and through discussions with the funders. These considerations need to be taken into account before biosecurity the risk assessment.

Strategies to lower the biosecurity risk (also for biosafety risk) of the laboratory work include:

- using in vitro propagation instead of in vivo models,
- using nucleic acid- and protein-based assays instead of in vitro propagation,
- conducting loss-of-function experiments instead of gain-of-function experiments,
- using synthetic or recombinant materials not sourced from the biological agent with biosecurity relevance,
- reducing the scale and/or scope of experiments,
- using attenuated strains or inactivated biological agents instead of wild-type isolates, or
- using molecular models such as pseudo viruses instead of in vitro propagation of the pathogen.

Strategies for the organization undertaking the research project regarding personnel involved in the project to lower biosecurity risk when working include:

- analysing different aspects of one project separately in different biological agents/strains, work conducted by independent teams instead of involving the whole team with all aspects of the project,
- Undertaking a computer-based (“in silico”) analysis instead of working in the laboratory with non-inactivated biological agents,
- limiting the number of personnel involved instead of including the whole team in all aspects of the project, and/or

- separating the project into confidential and non-confidential components with a limited number of personnel involved in the confidential part instead of including the whole team in all aspects of the project.

5.3 Types of laboratory biosecurity incidents

Biosecurity incidents include a range of potential threats that may pose risks to high-consequence materials, technologies, information, equipment and personnel. These can include, but are not limited to, the following incidents.

5.3.1 Incidents directly involving biological agents

Examples include:

- deliberate or accidental loss of biological agents,
- unintended or unauthorized release of biological agents,
- theft of biological agents or other biosecurity-relevant material and diversion during transportation,
- misuse of high-consequence material.

5.3.2 Physical security incidents

Examples include:

- unauthorized access to laboratory facilities,
- sabotage of laboratory activities and/or laboratory equipment,
- power outage, including back-up power,
- inappropriate use of equipment or infrastructure, or maintenance of laboratory facilities,
- break-in and intrusion,
- theft of devices, equipment or consumables.

5.3.3 Personnel-related biosecurity incidents

Examples include:

- biosecurity incidents caused by an insider (such as stealing),
- risks to personnel and facilities,
- non-compliance and other behaviours of concern.

5.3.4 Incidents related to information security and cybersecurity

Examples include:

- unauthorized access to or loss of information (digital or paper, such as personnel data, research data, genetic sequence data, standard operating procedures),
- discontinuation of operations due to cyberattack,
- unauthorized digital access to networked laboratory equipment,
- disruption of networked equipment (laboratory security system) through network connection,

- theft, misuse or sabotage of biosecurity-relevant information,
- espionage of biosecurity-relevant information.

5.3.5 Deliberate events

Examples include:

- terrorism,
- extortion in relation to high-consequence material.

5.3.6 Facilitating situations

There could be situations that facilitate biosecurity incidents based on the risk assessment, where risk control measures should be applied to prevent or intervene in their occurrences, such as:

- vandalism, picketing, occupation and barricading,
- labour issues and disputes, including workplace violence,
- strikes,
- civil unrest or war,
- facility and/or containment breach due to violent conflicts or natural disasters (for example, floods, tsunamis, earthquakes, tornados, hurricanes and mudslides),
- times with low personnel coverage.

5.4 Selecting the biosecurity risk assessment team

As suggested in subsection 5.1 Introduction, overlap should be minimized between people involved in high-consequence research and those carrying out the biosecurity risk assessment. Only persons needed to perform and review the research and the assessment should have access to material of biosecurity relevance. Roles and responsibilities of all members of the assessment team, as well as confidentiality issues, must be clearly defined before the assessment. Team members should have the necessary expertise for the assessment, commit to an institutional code of conduct, and sign a confidentiality declaration to ensure integrity and impartiality. Personnel undertaking a biosecurity risk assessment could include, for example, researchers, laboratory personnel, and facility maintenance or security personnel.

5.5 Risk assessment framework

The biosafety risk assessment framework (see *Laboratory biosafety manual fourth edition (2)*) was developed following a risk- and evidence-based approach to biosafety (Fig. 5.1). It aims to provide a basis for risk assessments with defined steps for institutions working with biological agents. This framework can also be applied for biosecurity risk assessments to comprehensively address biosecurity risks, implement risk control measures and review the measure regularly.

Fig. 5.1. Biosafety risk assessment framework

5.6 Biosecurity risk assessment steps

Based on the above-mentioned framework (Fig 5.1), an appointed team could perform a risk assessment for biosecurity-relevant work with the following steps: gather information; evaluate the risk; develop a risk control strategy; select and implement risk control measures; and review risks and risk control measures. Steps before the biosecurity risk assessment could include: a confidentiality declaration of the involved personnel; the application of strategies to lower inherent risks of high-consequence research; and an analysis of situations that could facilitate biosecurity breaches.

A biosafety risk assessment or a review of an existing biosafety risk assessment should also be carried out if high-consequence research or high-consequence material is identified in the biosecurity risk assessment and vice versa.

A decision tree for identifying high-consequence research is included in the gather information step of the biosecurity risk assessment template in Annex 1 (see Fig. A1.1). This decision tree is an adjusted version of that used to evaluate dual-use potential in the monograph on biosafety programme management *(27)*.

6 Biosecurity risk control measures

A biosecurity risk assessment will define risk control measures that will affect the laboratory's facilities and equipment, sample collection and transfer/transport, and/or define measures concerning the personnel involved. Furthermore, information that may be relevant to biosecurity requires appropriate biosecurity risk control measures.

For high-consequence research and work with high-consequence material, biosecurity risk control measures need to be implemented to enable the work to be conducted securely. In addition, research and laboratory work with material that does not meet the criteria for high-consequence research, referred in this guidance document as other biosecurity-relevant material, might be targeted with malicious intent. In this case, the consequences will likely be less severe (loss of reputation, economic damage) than if high-consequence research and/or material are targeted. Nonetheless, such biosecurity incidents also need to be prevented with the implementation of biosecurity risk control measures.

In this section, various risk control measures are presented for different biosecurity areas to enable facilities to implement locally effective and sustainable biosecurity risk control measures to manage biosecurity risks.

6.1 Personnel reliability, screening, recruitment, competence and training

6.1.1 Personnel reliability and biosecurity culture

Reliable personnel are crucial in laboratories working with high-consequence material with biosecurity relevance to reduce insider threats and prevent biosecurity incidents from within. Training programmes to raise awareness of biosecurity threats and how to respond to such incidents (including peer reporting) should be part of the laboratory's biosafety/biosecurity management programme. Peer reporting of other personnel who may pose a biosecurity risk is an important responsibility of the personnel. The procedure for peer reporting should also include a process by which any accusations are investigated and rebuttal is allowed for the person accused. Otherwise, the ability to report coworkers could be misused by personnel with an ulterior motive to attack guiltless employees.

A biosecurity culture comprises awareness and shared values and beliefs on biosecurity compliance. A code of conduct is an important part of the biosecurity culture of an institution. It goes beyond a soft regulation that sets standards of behaviour of personnel to encompass best practices of handling material, technology and information of biosecurity relevance and guidance for laboratory personnel on how to perform their work. Therefore, a code of conduct should be described in the biosecurity section of the institutional biosafety policy. All personnel working in the facility should follow the code of conduct. In certain situations it may be necessary for laboratory personnel to sign legally binding non-disclosure agreements which commits them to maintaining strict confidentiality and preventing them from disclosing sensitive information they may have knowledge of during their work.

The code of conduct should define norms and guidelines. It could include legally binding and locally suitable behavioural norms that regulate the work relationship between the personnel

and their attitude towards work and challenges. The 2021 *Tianjin Biosecurity Guidelines for Codes of Conduct for Scientists (29)* are a set of 10 guiding principles and standards of conduct designed to promote responsible sciences and strengthen biosecurity governance at national and institutional levels. The guiding principles relate to:

1. ethical standards,
2. laws and norms,
3. responsible conduct of research,
4. respect for research participants,
5. research process management,
6. education and training,
7. research findings dissemination,
8. public engagement in science and technology,
9. role of institutions, and
10. international cooperation.

Research institutions and governments are encouraged to incorporate elements from the Tianjin biosecurity guidelines in their national and institutional practices, protocols and regulations to minimize the risk of misuse of high-consequence research and material, technology and information. The WHO guidance framework for the responsible use of the life sciences *(7)* identifies a common set of nine values and principles that are viewed as benchmarks for considered ethical judgements to support the development and implementation of effective mechanisms for biological risk management. These values and principles are:

- health, safety and security,
- responsible stewardship of science,
- integrity,
- fairness,
- openness, transparency, honesty and accountability,
- inclusiveness and collaboration,
- social justice, and
- intergenerational justice.

The values and principles underline the need for the scientific community and other stakeholders associated with life sciences to adhere to high scientific and ethical standards, and to ensure that life sciences research and developments are used for the betterment of humans and the Earth's biodiversity, ecosystems and environments. They are intended to motivate and strengthen ethical and responsible practice, and to guide the policies and actions of WHO Member States and other stakeholders.

It could be challenging to detect violations against the institutional code of conduct as they depend on an individual's attitude and motivation. Nonetheless, potential violations should be dealt with to ensure the responsible handling of high-consequence material. The process for dealing with violations should be outlined as part of the code of conduct or in the institutional biosecurity policy.

6.1.2 Personnel screening, recruitment, monitoring, support and protection

For assessed high biosecurity risks, personnel need to be comprehensively screened, either uniformly or proportionately according to their roles and accessibility to high-consequence material and the facilities that contain them. Personnel screening aims to identify individuals who may be at greater risk of assisting or contributing to biosecurity incidents.

Initial personnel screening should be conducted before the recruitment of candidates, in cooperation with the human resources department and other divisions as applicable. In job advertisements, potential candidates should be made aware that background checks and other verifications are necessary. All aspects of the personnel reliability programme should be listed in job advertisements, with position descriptions and even codes of conduct, where appropriate (if working on high-consequence research or with high-consequence material). In addition to formal qualifications, job candidates should have a background check concerning their behaviour and physical suitability for the job.

Personnel screening does not end with the recruitment of a suitable individual. Regular checks and continued monitoring of the employee should be performed by supervisors. The frequency of this monitoring will depend on the institution. Any behavioural changes should be monitored by coworkers and supervisors to prevent potential biosecurity incidents. Additionally, mechanisms should be in place to enable anonymous reporting and no-fault reporting of any concerns about behaviour (or about coworkers) to laboratory or line management. A culture of responsibility must be ingrained through continual training and communication.

The biosecurity risk assessment should also consider and identify all personnel with direct or indirect access to high-consequence material, including, but not limited, to laboratory personnel, scientists, students, information technology personnel, engineers, transport personnel, laboratory support personnel, and operations and maintenance personnel, whether internal, external or ad hoc.

In the biosecurity section of the institutional biosafety programme, institutions should define the scope of screening that needs to be performed periodically for the particular personnel. This type of screening should be conducted for items that could change over time or if there are changes in roles and responsibilities. Table 6.1 lists the types of screening and the items to be considered for personnel screening. The items may vary for support and ad hoc personnel. Institutions must also define a process and procedure so that candidates from other countries are not disadvantaged as security screenings might be difficult to obtain and assess. The screening process will depend on the institution´s activities as well as the characteristics of the materials that are received, manipulated, stored, used and/or transferred.

Table 6.1. Screening items for potential candidates for recruitment and for existing personnel

Type of screening	Screening items for candidate recruitment	Screening items for existing personnel
General background screening	• Curriculum vitae • Job interview • Letters of recommendation or performance reports from former employer(s) • Breaks in education or working life • Verification of credentials	• Previous performance reports if new responsibilities will be assigned that need other security checks • Semi-annual safety screenings, agent handling spot checks, review of active participation in protocols
Security-related screening	• Association with organizations that could present a threat to the integrity of the facility • Unwanted beliefs and/or participation in certain action groups • Previous involvement in scientific misconduct or fraud • Conflict of interest that could present a risk to the impartiality • Responsibilities in a previous job (such as handling high-consequence material) • Criminal records, police reports and financial probity • Misuse of/dependency on drugs and alcohol • Concerning activity on social networks • Certain medical conditions, both behaviour-based and physical, that could lead to unstable or undesirable behaviour	• Association with organizations that could present a threat to the integrity of the facility • Conflict of interest that could present a risk to impartiality • Criminal records, police reports and financial probity • Misuse of/dependency on drugs and alcohol • Concerning activity on social networks • Medical conditions, both behaviour and physical, that could lead to unstable or undesirable behaviour • Observed non-compliance with a code of conduct
Screening tests	• Personality tests based on the job requirements • Psychological behaviour assessments • Medical checks	• Psychological behaviour assessments • Medical checks

Personnel working in sensitive projects or sharing of biosecurity-relevant information may become relevant to biosecurity, and may need their anonymity to be maintained and personal protection to prevent sensitive information being shared if targeted and manipulated by techniques such as social engineering. Therefore, a system should be set up for personnel support and protection, including policies, procedures and training programmes.

Furthermore, it is important to establish a culture that ensures individuals feel trusted and are able to discuss all issues and to provide support for personal problems such as financial issues, medical concerns (mental or physical health), and drug or alcohol misuse.

6.1.3 Personnel competence and training

To inform and enable laboratory personnel and other employees to act appropriately in biosecurity-relevant situations, biosecurity education needs to be provided when new personnel join the institution and periodically as set out in a training plan.

Personnel competence is a combination of qualifications, training, skills and experience. The required qualifications and experience for each role are specified in the job description, and personnel are selected accordingly to match the requirements. However, biosecurity is not part of the curriculum of many qualifications and there will also be site-specific information. Therefore, job-specific training and mentoring will be needed until a person becomes competent in their tasks and to ensure compliance with the biosafety/biosecurity programme. Competency can be assessed through a combination of education, training, examinations, observation and regular performance evaluations.

An assessment should be made about the need for biosecurity training for laboratory personnel, students, scientists, managers, facility maintenance personnel, shipping personnel, security leads and facilities managers, and this should be incorporated in a training plan. The types of personnel who need biosecurity training may differ depending on the size of the facility and the type of laboratory work being conducted, for example, doing high-consequence research. Initial training should be given to all personnel to raise awareness about their duties to protect the security of the assets. More specific and detailed information about assets and response plans should be given on a need-to-know basis.

A training plan must be suitable for the different roles within biosecurity and it may need to consider national requirements. The plan must state what training the different roles should receive, how frequently, and how the training will be delivered and documented. The training curriculum should contain the appropriate information for each role, taken from:

- the biosecurity risk assessment,
- biosecurity risk control measures,
- biosecurity best practices,
- types of biosecurity incidents and their consequences, and
- incident response to biosecurity incidents.

Areas of training include, but are not limited to:

- handling and storing high-consequence material and other biosecurity-relevant material,
- laboratory techniques,
- identification of misinformation/disinformation,
- Identification of high-consequence research,
- bioethics related to the work with high-consequence material,
- biological weapons,
- biosecurity risk assessment training,
- relevant national/international regulations,
- responsible conduct of research and application of the life sciences,

- supportive team working,
- reporting, follow-up and investigation,
- training on insider threats,
- cybersecurity and information security,
- identification of manipulation (for example, social engineering),
- transfer and transport of high-consequence material,
- storage, inventory accountability and management of high-consequence material,
- final disposal, infectious waste management and associated records,
- tabletop drills of biosecurity incident response, and
- emergency response training (for example, handling critical situations directly related with biosecurity).

6.2 Physical security

Physical security measures are biosecurity (and biosafety) risk control measures to ensure personnel can work safely and securely in the laboratory, and access of persons to the laboratory is authorized, regulated, controlled and stopped, if necessary. Furthermore, physical control measures aim to prevent theft, misuse and sabotage of high-consequence material.

6.2.1 Facility security and access regulation

Passive physical security

A passive security system is a physical security risk control measure that is not monitored and does not require or provide an immediate response, but still requires maintenance and upkeep. Generally, passive security is a significant deterrent to prevent access of unauthorized individuals to secure premises, facilities and equipment, or theft of high-consequence material. Furthermore, passive security could provide a means of supervision of personnel, which might prevent or detect biosecurity threats by insiders.

In the context of laboratories, passive security risk control measures to prevent intrusion or loss of biosecurity-relevant material, technology and information could include the following:

- passively controlled/monitored entry and exit, for example, radio-frequency identification cards, keys,
- perimeter fences and walls around the laboratory facility,
- sufficient illumination to deter night-time entry from the external environment into laboratory premises,
- conventional alarm systems and closed-circuit television systems,
- Lockable laboratory storage equipment (for example, freezers, refrigerators, storage cabinets for materials),
- sealed windows,
- lockable doors at all access points,
- tempered (toughened) or bullet-proof glass in windows,
- sufficient and sustained power sources or generators to maintain electrical security systems,

- security system with layered permissions and more advanced access systems such as fingerprint or iris scan, and
- ram-proof barriers or bollards.

Passive security systems would be implemented with layers of access depending on the risks associated with the facility. Compared with laboratories with other biosecurity-relevant material, higher risk would be considered for:

- laboratories handling or storing high-consequence material, and/or
- laboratories with equipment, devices, technology or information of biosecurity relevance.

Access to restricted areas is required for certain individuals such as scientists or other personnel who have received security clearance. Access to restricted areas of laboratories by others would require permission and escort by an individual trained in and cleared for security.

Active physical security

Active physical security measures are a type of physical barrier implemented through active surveillance or intervention by one or more individual or system. Examples of active physical security measures could include:

- security services or guards,
- requirement to check in at reception or front office,
- motion detectors or anti-intrusion devices,
- video surveillance monitored by security guards,
- active security alarm monitoring (for example, with anti-intrusion devices),
- firewalls on computer systems,
- requirement to record personal details of visitors and guests,
- access to restricted areas based on security clearance,
- denial of access or escort to sensitive areas for unauthorized personnel,
- emergency/incident response and preparedness training and exercises, and
- auditing and monitoring of access control system and user activity on the information system.

Controlled access to laboratory areas

While passive security measures prevent unrestricted access to sensitive areas, at times some personnel or visitors will require access to these areas. The way such access can be regulated is through controlled access.

Depending on the nature of the individuals requiring access to sensitive areas of the laboratory and the biosecurity-relevance of the area, the process may require significant administrative oversight to ensure security is maintained. People who may be permitted access to sensitive areas of laboratories could be:

- laboratory personnel who handle the high-consequence material and/or carry out laboratory activities regularly or routinely with other biosecurity relevant material;
- personnel who provide laboratory support services (such as maintenance personnel);
- attachment personnel, for example, visiting researchers, laboratory auditors or students on attachment to perform laboratory activities;

- visitors, who do not carry out any laboratory work and are in the laboratory for short and defined periods of time such as
- facility maintenance and repair personnel,
- delivery personnel, and
- trainees and students.

For all these groups of people who could access high-consequence material, access procedures, accompanying personnel and supervision must be provided.

To ensure no breach of the layers of security, personnel need to be trained regularly on awareness and requirements for entry, including for guests and visitors. This training would include the requirement for administrative clearance, including documentation and credentials, and information on what to do in case of emergencies.

Furthermore, for visitors, non-staff or non-regular personnel, the following areas need to be addressed in the biosafety/biosecurity policy:

- measures for awareness-raising of personnel of biosecurity issues,
- training for attachment personnel (for example, maintenance personnel),
- responsibilities of personnel (biosecurity risk control measures),
- procedures for allowing access for visitors, including what information to record,
- identification, registration (entry and exit) and signing,
- accompanying personnel and timeframe,
- defining legitimate purposes of visiting,
- condition of the facility during the visit (for example, without current laboratory work and decontaminated),
- preparation in the laboratory when expecting visitors, and
- definition of accessible and inaccessible areas for visitors.

6.3 Inventory control and laboratory equipment

6.3.1 Laboratory inventory

Laboratories that store or handle biological agents should keep an updated list of all materials/products that are present in the facility as a best-practice to monitor the location and volume of such products that are always present. For biosecurity-relevant laboratory equipment and/or information, the inventory list may also include laboratory devices, consumables, kits, instruments, reagents and even data with all risk control measures and standard operating procedures applicable. Inventory documents need to be securely handled, properly maintained and regularly audited. Any discrepancies should be investigated and resolved. For equipment, devices and kits, a detailed record of relevant information should be kept, including a logbook of usage and decontamination processes and an archive of data generated.

A laboratory inventory system needs to be accompanied by a biosecurity risk assessment, and risk control measures should cover:

- access control,
- responsible personnel,

- training of personnel,
- record keeping,
- frequency of inspection,
- functional examination (quality tests, for example, polymerase chain reaction for DNA quality evaluation and culture for microorganisms),
- reporting system for biosecurity breaches,
- audits (internal and external) and inspections,
- specialized standard operating procedures, such as removal of biological material from the inventory by two employees, which reduces errors during removal,
- amount of information that must be entered into the inventory system for each sample.

The inventory of high-consequence material should be treated as sensitive information and be stored separately from other biological agents, with access given to only a small, selected number of people. Digital inventory databases must be protected and access must be limited to certain specific individuals. Layered physical access and additional biosecurity risk control measures, such as locked refrigerators and/or freezers, should also be implemented for storage of high-consequence material. Any discrepancies in the recording must be investigated and reported to appropriate authorities as possible or suspected theft or loss.

A facility-specific approval system for use of high-consequence material needs to be established, which should include justifications and documentation for research, propagation, inactivation, transport and disposal of material.

6.3.2 National inventory

The safe and secure storage of regulated high-consequence material can be recorded in a national inventory to ensure proper handling, packaging and storage. As well as the responsible national authority, other stakeholders involved in national inventory are legislative authorities and repositories/laboratories that store the high-consequence material and their IBCs.

Most approaches to a national inventory are based on a national or international list of regulated/restricted high-consequence materials for which the national authorities responsible aim to apply storage and handling requirements. At the national level, a selection process of laboratories might be reasonable to identify qualified institutions and limit the number of facilities storing and handling certain high-consequence material for which an oversight mechanism needs to be established. As an international recommendation, the WHO Joint External Evaluation tool (based on the IHR) *(5)* recommends minimizing the number of facilities with high-consequence material.

A risk-based approach to establishing a national inventory informed by a biosafety and biosecurity risk assessment includes reviewing novel research results of the biological agents as soon as they become known. New information on unknown pathogenic features of the biological agent or identified high-consequence research may require the biosecurity risk control measures to be revised. In the hybrid approach described in subsection 8.1.2 on risk assessment, a national authority, for example, requests a national biosafety committee (a national committee of independent experts on the subject) to evaluate high-consequence materials included in a national inventory which is regularly updated.

To establish a national inventory, the following elements need to be provided by the national regulatory body:

- oversight and requirements of laboratories involved (surveys, inspections, reports),
- biosafety and biosecurity risk assessment for the restricted high-consequence material,
- funding for biosafety risk control measures and biosecurity risk control measures,
- criteria for selection of laboratories to participate in a national inventory system,
- a recommended or required scheme for the inventory, and
- internal inventory management and external inventory control.

6.4 Destruction, decontamination and waste management

When conducting daily laboratory work, reliable methods for decontamination and destruction, as well as an appropriate waste management plan that assigns accountabilities, must be available for all biosecurity-relevant material, technology and information, such as biological agents, laboratory equipment and information. After the decontamination necessary within the biosafety requirements *(30)*, destruction of the high-consequence material might also be necessary if determined by the biosecurity risk assessment. Furthermore, security around high-consequence material, particularly information about biological agents and equipment used for propagation and storage, must be maintained until the security risk has been eliminated with the decontamination and/or destruction. The following factors need to be considered with implementing risk control measures related to decontamination and destruction:

- personnel involved (for example, laboratory personnel, technicians and operators),
- transfer, transport and storage of waste,
- standard operating procedures,
- recording and monitoring (for example, process of decontamination and/or destruction, autoclave (mal-)function and tracking system), and
- validation of methods (for example, with bioindicators and/or polymerase chain reaction).

6.4.1 High-consequence material

Residual, high-consequence material of biosecurity relevance, including, DNA, toxins or other biological structures, may remain or be left after use. In some cases, the best way to destroy this material should be assessed before work begins and during the biosecurity risk assessment. The destruction could be achieved by a combination of validated processes (for example, disinfection, autoclaving or incineration) to ensure that the high-consequence material cannot be recovered and no information from the destructed material can be extracted. The items for destruction could include:

- microorganisms,
- genetic material,
- other biological structures such as proteins and toxins,
- any labelling of the receptables, and
- receptacles that has been in contact with the high-consequence material.

6.4.2 Laboratory equipment, devices, information and software

In the course of the laboratory work, residual high-consequence material or other biosecurity-relevant material could left on a device or equipment. This material could pose a biosecurity risk

even though the organism is not viable, for example, DNA, toxins or other biological material. In addition, the device or equipment itself could have biosecurity relevance; for example, it could be used to synthesize biological material, such as restricted DNA sequences from high-consequence pathogens, or a biological agent that could be used as a toxin. Therefore, before disposal, laboratory equipment or devices should be decontaminated by validated methods to prevent unintentional exposure or release of biological agents and to remove any biological material from the device. Furthermore, a device with biosecurity relevance, as a whole or a critical part of it, needs to be destroyed in a validated process to prevent unauthorized or malicious use. A record must be kept of all equipment disposal, including details of the equipment, and the decontamination and disposal methods used.

All laboratory equipment and devices relevant for biosecurity should be part of the biosecurity risk assessment. As computer hardware (or devices that store data) could contain information or software of biosecurity relevance, no relevant data should be left on the hardware or software that could be used for malicious intents, and removal of these data must be assured.

Sensitive information about high-consequence pathogens (such as name, storage location, nucleic acid sequence and quantity) may be stored on paper, hard drives, laptops, emails and servers. It is important to ensure that each type of information is kept secure until disposal by having audited waste routes for paper destruction, destruction of hard drives and secure well maintained data storage.

Deleting information from a computer or digital storage device does not mean the data cannot be retrieved. Old, unwanted, outdated and discarded electronic devices pose a biosecurity risk, and a process to render the data unrecoverable should be in place.

6.5 Information security and cybersecurity

Every laboratory produces electronic information. Most of this information should not be disseminated unrestrictedly and some information needs active protection. In this subsection, the control of information and possible biosecurity risk control measures to prevent theft, leaks and misuse of information are addressed. In addition, malicious cyberattacks *(31)* can occur and effective risk control measures needed to prevent them are discussed. Furthermore, possibilities for secure access to data (digital and paper) and safe sharing of information with colleagues or other parties will be addressed.

Based on a local biosecurity risk assessment, information with biosecurity relevance could be, but is not limited to:

- data stored in the laboratory or computers in offices belonging to the laboratory,
- internal documents (for example, data and printouts),
- communications (for example, emails, voice mails, memos and conversations),
- unpublished research results,
- standard operating procedures, laboratory workflows and protocols,
- software/programmes,
- inventory lists,
- nucleic acid sequences (for example, of pathogens, including whole genome, genes, antibiotic resistance mutations, primers and RNA guide sequences),
- passwords and usernames,

- intellectual property and patents,
- internal information stored externally or in other departments of the institution (for example, information about personnel including medical reports and personnel performance reports, and laboratory layout plans),
- laboratory logbooks containing details of the research activities, and
- systems for inventory storage, building management and automation.

Biosecurity incidents related to information about high-consequence material could include:

- unauthorized access to information (for example, digital or paper including personnel data, research data, sequence data and standard operating procedures),
- misuse of information,
- cyberattacks on facility systems,
- loss or theft of biosecurity-relevant information,
- phishing,
- espionage of biosecurity-relevant information (also personal data via social media), and
- unauthorized use of electronic devices.

Similar to physical security, data protection and cybersecurity include regulated physical access to information, for example, digital and physical access to computers/devices, including laboratory equipment with network capability, password protection of information and regulation on data on portable devices.

Information with biosecurity relevance is identified by the biosecurity risk assessment and requires biosecurity risk control measures. Those measures are outlined in the following subsections.

Physical risk control measures

- regulation of physical access to buildings or areas with relevant information and restriction to authorized personnel,
- physical security measures for accessing data (for example, multilayer password, key to enter the room, authorization for access to biosecurity-relevant information and regulations on sharing this information),
- restriction of physical access to biosecurity-relevant information to defined/selected personnel,
- protection of equipment with biosecurity-relevant information (for example, computers, servers, but also laboratory devices with access to the laboratory network).

Personnel-related risk control measures

- background checks on responsible personnel,
- appropriate personnel training (for example, on social engineering),
- restricted access to controlled areas for personnel who are under investigation.

Electronic risk control measures

- passwords,
- two-stage authentication,
- protective programmes (that is, firewalls),
- electronic protection of the connection to a laboratory network or internet,
- data backup,
- measures to prevent cyberattacks in teleconferences.

Administrative risk control measures

- selection of the physical location to store biosecurity-relevant information (for example, external service provider, email, clouds, server and cooperation partner),
- policy for handling biosecurity information outside the laboratory, for example on (private) laptops and avoidance of using public Wi-Fi,
- regular change of passwords and avoidance of reusing highly similar passwords *(32)*
- use of a different password for each login into a separate account,
- policy on the handling of intellectual property,
- risk control measures to prevent cyberattacks not only on computers and data, but also on electronic key systems, building management/automation systems, and camera/intrusion detection systems (linked to physical security),
- policy on best practices to handle biosecurity-relevant information securely (for example, hard disk, email, USB stick, back-up and encrypted storage devices),
- ban on external storage devices in the working area unless officially permitted for work,
- policy on data transfer security (for example on information sharing via email, databases and websites),
- emergency response in case of a cyberattack,
- emergency response for disaster recovery (data back-up),
- penetration/vulnerability test,
- maintenance of an offsite data back-up storage location,
- ban on personal electronic devices in areas with sensitive information,
- cybersecurity training (for example, identification of emails with malicious content/ attachments and identification of social engineering),
- validation of procedures and tools for preventing cyberattacks, including communication paths for collecting and disseminating information on cyber incidents and situational awareness, response and recovery,
- destruction of information on out-of-use devices,
- policy for online ordering.

How to create and use a secure password – a suggestion

- Use 10 characters minimum with capital letters, numbers and special characters.
- Use a different password for each log-in.
- Use an easy to remember, hard to forget password, for example, a combination of two words, the beginning of one word and the ending of another word, plus a number with a personal relation and a special character.
- Do not note the password on paper or digitally unless your institution has adopted a secure password management software.
- Change password regularly.

6.6 Emergency/incident prevention and preparedness

Biosecurity incidents in laboratories handling or storing high-consequence material need tailored responses informed by the biosecurity risk assessment. Biosecurity emergency response plans for facilities handling or storing high-consequence material need to consider the following:

- envisaging scenarios or types of potential biosecurity threats that will require an emergency response;
- developing and validating standard operating procedures for a biosecurity emergency response in advance, taking account also of associated hazards, for example, chemicals;
- training requirements, including periodic refresher training and exercises, ideally done in person;
- mechanisms to report, record and investigate incidents, communicate the lessons learnt, and track the implementation of lessons learnt;
- crisis/incident communication;
- coordination mechanism with external emergency and security responders, including risk communication, regular training and exercises to enhance emergency response interoperability;
- salvage policy/procedures and potentially external bodies to be involved.

Biosecurity threats could be incidents or emergencies. A near miss is defined as an incident that does not have adverse consequences but needs to be reported so systems can be improved to prevent future incidents. Some incidents may not be identified or discovered immediately but sometime later. Furthermore, not all biosecurity incidents may happen on-site. Reporting protocols should also include the possibility of reporting a suspected biosecurity incident, such as a lost or stolen security pass.

Similar to biosafety incidents, biosecurity incidents or emergencies might need cooperation with local emergency agencies, for example, firefighters, law enforcement agencies, ambulance services and emergency departments. External authorities, such as law enforcement, might also need to be involved in developing emergency plans and investigating biosecurity breaches.

In Annex 2, biosecurity emergency response templates are provided that can be customized to local circumstances.

6.6.1 Reporting, investigation and corrective actions

A programme needs to be established whereby biosecurity-related events are reported, investigated, and corrective actions implemented to support a risk management system.

In safety, near misses do not result in injury or death, in biosecurity, near misses may be not result in release (intentional or unintentional) or loss of high-consequence materials. Examples of near misses include lost security pass, suspicious personnel loitering around the laboratory premises, personnel showing particularly keen interest in the whereabouts of biological agents or equipment in laboratories, or failure of a security door lock system.

Near misses or other incidents that do not result in immediate loss should be reported, reviewed, classified and analysed for any common links. Once the contributing factors are identified, appropriate corrective action, such as a case study during refresher biosecurity training, should be taken.

In addition to reporting and responding to near misses and minor incidents, plans to prevent and mitigate low-frequency but high-severity events should be reviewed.

Low-frequency but high-severity events could include complete loss of power to the site with failure of back-up generators, intruders on site at weekends, or reports of specimens from a laboratory found in the community.

6.6.2 Emergency destruction of high-consequence material

Rare situations may arise when it is necessary to rapidly destroy biological high-consequence material or other material of biosecurity relevance to prevent a biosecurity incident. Before the response can start, a process document, provided by the appropriate authority, must be in place that describes the situations (such as natural disasters, violent attacks to facilities), the personnel, equipment and first steps to be taken. This document should be reviewed regularly and updated during the biosecurity risk assessment.

The following elements may inform the biosecurity risk assessment for the emergency destruction of high-consequence material:

- analysis of the local circumstances such as political situation, civil unrest and/or war or the vulnerability to natural disasters (such as earthquakes, tsunamis, floods and/or fires) based on past events or the geographical location;
- consideration of the minimum number of personnel required for the emergency destruction of the high-consequence material and/or information;
- determination of which items (high-consequence or biosecurity-relevant samples, devices, equipment, software, protocols or data) may require emergency destruction, and how to prioritize the items for destruction (order of destruction);
- identification of risk control measures that could be implemented in addition to the destruction of the biosecurity-relevant material to prevent unauthorized access to the high-consequence material and/or other biosecurity-relevant material.

A decision-making tree may help to identify the most suitable action in an emergency and could include the following elements:

- potential situations that would trigger an emergency destruction of high-consequence material,

- high-consequence material that would need to be inactivated or destroyed in a specified situation,
- necessary personnel, equipment, devices and standard operating procedures, and
- situational circumstances such as no electric supply.

Furthermore, the following aspects should be considered.

- Standard operating procedures for the safe and secure emergency destruction of biosecurity-relevant material must be validated and be able to be performed at any time.
- Devices for the destruction of high-consequence material, for example, an incinerator, need to be ready to use. The turnaround times for one load need to be considered in the emergency destruction plan as well as prioritization of samples for destruction.
- Personnel and replacement personnel need to be identified and trained to carry out the emergency destruction. Training for other relevant personnel and development of standard operating procedures and alternative destruction methods (for example, in case of no electric supply) need to be considered.
- Exercises, such as tabletop and mock-ups, should be carried out to ensure an understanding of the steps in emergency destruction of biosecurity-relevant materials.
- Once such a situation has occurred, the event needs to be documented and analysed, and adequate destruction of the high-consequence material needs to be demonstrated and validated as far as possible.

7 Transfer and transport of high-consequence material

High-consequence material can be transferred or transported inside a facility, between facilities, within a country and between countries and continents.

All persons involved in the transportation or transfer must follow secure and safe working practices, ensuring that the high-consequence material is secure and safe at all times, and adhere to biosecurity risk control measures. The likelihood of theft, loss or damage and/or release of a high-consequence material from a secure environment and the repercussions of a deliberate release are both considered in the biosecurity risk assessment.

Policies, standard operating procedures, practices and procedures, such as material transfer agreements, have been designed to reduce the risk of insider and outsider threats during transit. Transport security serves as a control system to reduce the danger of theft from inside and outside while high-consequence material is transported between different jurisdictions.

7.1 International agreements

For the transport of high-consequence materials (for example, infectious substances with biosecurity relevance), no dedicated international legislation or agreement currently exists. The biosecurity of infectious substances during transportation is important. A chain of custody should be applied to monitor the high-consequence material during transport. Furthermore, several relevant guiding documents have been published by the United Nations (UN) and WHO.

The UN Model regulations set out the requirements for the transportation of dangerous goods, including infectious substances (Category A, Infectious substance UN2814 and UN2900 or Category B, Biological substance UN3373). Other relevant documents with varying relevance in certain parts of the world include the current *Agreement concerning the international carriage of dangerous goods by road* (ADR) *(33)*, *Regulations concerning the international carriage of dangerous goods by rail* (RID): *applicable as from 1 January 2023 (34)*, the *International maritime dangerous goods (IMDG) code (35)*, *Technical instructions for the safe transport of dangerous goods by air (Doc 9284), 2021–2022 edition (36)*, *Technical instructions for the safe transport of dangerous goods by air (Doc 9284), 2023–2024 edition (37)*, and *Guidance on regulations for the transport of infectious substances 2023–2024 (38)*.

7.2 National legislation for the transport of high-consequence material

In general, national legislation related to the transportation of high-consequence materials is based on the UN model regulations and aims to ensure that these are transported safely and securely to prevent any accidental or deliberate release, resulting in exposure to these materials. The specific regulations governing the transportation of infectious substances can vary considerable by country, but they typically cover proper packaging, labelling, documentation and training for those involved in the packing and transport process. These regulations focus

mainly on the biosafety aspect of transport. Biosecurity considerations are described in subsection 7.3, and more information on export control can be found in section 8.

7.3 Biosecurity for the transfer and transport of high-consequence material

7.3.1 Fundamentals

- Implementation of material control and accountability will diminish the risk of insider and outsider threats during the transfer of biological material within a laboratory facility, institute, country or internationally. A properly maintained inventory system is mandatory for safeguarding infectious substances.
- Accountability and responsibility at each step enhance the secure transportation of the high-consequence material; relevant documentation and oversight are imperative.
- Not all high-consequence material or biosecurity-relevant material is classified as infectious substances (Category A). These are: exemptions (for example, nucleic acid), biological substance (Category B), and exempt human/animal specimens *(38)*.
- The nominated/appointed officer for the shipment of infectious substances has to be formally approved for this activity. If there are no available couriers, the transfer will need to be discussed and prepared by the interested parties in the transfer (for example, institutions and regulatory bodies).
- During transportation, high-consequence materials are more prone to tampering or theft. Implementation of biosecurity measures for transportation will reduce inappropriate handling of the materials by laboratory personnel, theft or misplacement.
- It is important to ensure that only authorized personnel have access to high-consequence materials.
- Confidentiality or security of information is a prerequisite to ensure laboratory/institutional biosecurity.

7.3.2 Requirements

- The inventory must be properly maintained by laboratory personnel and regularly audited by the authorities or other authorized personnel. It should include a proper record of all the high-consequence materials withdrawn or added.
- A packaging list must be added to the shipment.
- Chain of custody must be maintained by different mechanisms including documentation (paperwork) and computerized or personal digital assistant scanners.
    - Standardized documentation, is obligatory. This documentation includes the name of the high-consequence material and its quantity (which has an upper limits), date and time of the dispatch, and complete contact information of the sender and receiver. It must have the signatures of the responsible officers.
    - The documentation moves with the high-consequence material during transfer or transport.
    - If it is not possible for the authorized individual to ensure custody of the package because of conflicting activities, then the package must be retained in the restricted access area with access control.

    - Temperature monitoring in the shipping container may need to be added.
- Shipping personnel are designated and well trained in proper packaging according to the standard operating procedures/regulations/standards. They must undergo refresher courses at regular intervals.
- Transfer or transport should be preapproved by the designated biosafety officer or designated responsible official in the institute and transfer approval records must be retained.
- Necessary permits must be obtained in advance of the shipment and additional local/state/provincial regulations for local/national/international transport must be adhered to.
- The details of the recipient (point of contact) must be known, endorsed in advance and contact details provided.

Additionally, in the case of transport, to transfer custody to a commercial courier the following requirements apply.

- Due diligence is required during all the stages of transport: preshipment, during transit and at the receiving end.
- Preshipment authorization depends on the nature of the high-consequence material to be transported and the appropriate authorization should be obtained.
- The responsible individual may be empowered to make shipping decisions for the non-restricted agents.
- The nominated/appointed officer must be formally approved for the shipment of high-consequence materials.
- A documented process for rapid destruction that could be necessary, for example, in emergency situations) of the material must be established and should include descriptions of the personnel and equipment needed to conduct the task.
- The packaging must have only the required standard information and labels and should include contact information of an expert who can advise first responders in case of damage to the shipment in transit.
- Digital tracking (such as global positioning system tracking devices) should be used to provide a constant trail of the location of the material. Personnel can be trained on tracking and monitoring during transport.
- Tamper-proof security tapes with serial numbers should be used to help detect any tampering of the package.
- The responsible recipient personnel must be informed beforehand about the shipment of high-consequence material.
- Once the shipment has been received, the responsible recipient personnel, should hand over custody to the authorized personnel for inventory verification and storage. In addition, the sender must be immediately informed through the established method that the delivery has been received.
- Standard operating procedures and preparation must be in place at the sending and the receiving facilities in case of any delay or if the package does not arrive as expected, or if any anomalies or tampering are observed, such as damage to the third layer of packaging *(2)* and/or leakage.

- Law enforcement authorities or other relevant governmental agencies should be well trained and informed immediately if some high-consequence material is found missing or if any tampering during the transport is observed.
- If a package of high-consequence material is received without prior information, the biosafety officer and/or security personnel of the receiving institution must be informed.
- Safety regulations and policies restrict the amount of dangerous goods that can be transported and this restriction must be observed. This limitation provides security benefits during transport.
- No information should be shared with other persons not involved in the transfer or transportation once high-consequence material is shipped.
- The sender needs to consider that the outer packaging *(2)* of international air freight might be opened to top up refrigeration agents (for example, dry ice) during transit, so information about the content should not be visible when opening the outer packaging. If there is a need to replenish the coolant material, this should be stated in the transport documents.

7.3.3 Personnel

A rigorous selection process, background checks, security clearance and regular monitoring are mandatory for the personnel responsible for shipment/transfer of high-consequence materials. Continuing professional training is required to maintain competence of these personnel *(39)*. These personnel include all those responsible for packaging, sending and receiving of high-consequence materials, inventory control and laboratory managers, and they should be considered in the biosecurity risk assessment. An example of a risk control measure related to personnel is the requirement for the involvement of two persons in critical steps in the shipping process.

7.3.4 Material transfer agreements

A material transfer agreement is a legal contract that governs the transfer of biological, chemical or other laboratory materials from one institution to another. These agreements are often used in scientific research to ensure that the recipient of the materials agrees to use them for a specific purpose and to follow certain conditions.

Material transfer agreements typically define the scope of the transfer, including the quantity and nature of the material being transferred, as well as any limitations on the use or distribution of the material. They may also specify the rights and responsibilities of both the provider and recipient of the material, such as confidentiality obligations, intellectual property rights and liability for any harm resulting from the use of the material.

The terms of a material transfer agreement can vary widely depending on the nature of the material being transferred, the purposes for which it will be used, and the preferences of the parties involved. Factors to consider for a material transfer agreement *(41)* include:

- the provider and recipient of the high-consequence material,
- rights and obligations of the provider, the recipient and any other involved party,
- aim and background of the provision of material,
- intellectual property rights,
- warranties and responsibilities,

- term, amendment and termination conditions,
- notifications and communication,
- dispute resolutions, no waiver of privileges and immunities and final provisions,
- information about the high-consequence material,
- policy about the publication of information about or information generated using the high-consequence material,
- requirements for transfer and transport,
- specifications for the final disposal or retention of the material, and/or
- biosafety and biosecurity requirements for the recipient.

7.3.5 Transfer and transport of equipment with biosecurity relevance

Regulation of the transfer and transport of equipment with biosecurity relevance aims to prevent the misuse of such items for harmful purposes, including the development or production of harmful biological material or even biological weapons. The specific regulations governing the transfer and transport of such equipment can vary substantially by country, but they typically require proper documentation and licensing, as well as training for those involved in the transfer and transport process.

When transporting biosecurity-relevant equipment, due diligence should be taken to ensure the equipment has been properly decontaminated, packed and secured, and that the receiver has the required security measures in place and is properly trained for its use. Examples of equipment with a biosecurity relevance include sequencers, incubators, bioreactors and primary containment devices *(16)*.

8 National and international legislation and regulation

The development, implementation and oversight of risk-based biosafety and laboratory biosecurity procedures are essential for working safely and securely with high-consequence material that pose serious risks to human, animal and plant health, and animal and plant products. For the past few decades, emphasis has been placed on working safely with biological agents, particularly with the publication of the fourth edition WHO's laboratory biosafety manual *(2)*, the sixth edition of the Centers for Disease Control and Prevention's *Biosafety in microbiological and biomedical laboratories (42)* and the third edition of the *Canadian biosafety standard for facilities handling and storing human and terrestrial animal pathogens and toxins (43)*. This has not been the case for laboratory biosecurity. Many countries are in the process of updating or developing national legislation for biosecurity. A number of countries have legislation covering some of the elements of laboratory biosecurity, with implementation and oversight often lagging far behind. Risk- and evidence-based overarching international biosecurity legislation/regulation will help both regulated and less regulated countries to shape their national legislation/regulation on working with high-consequence material as safely and securely as possible.

In this section, national and international legislation/regulation to support laboratory biosecurity of high-consequence material are presented, and best practices for national legislation/regulation are provided. In Annex 3, examples of national legislation in biosecurity are outlined.

8.1 Best practices in national legislation and regulation on biological risks

High-consequence research and handling or storing of high-consequence material need to be covered by legislation to set national requirements on safe and secure laboratory work. The aim of biosafety and laboratory biosecurity legislation/regulation is to support the continued progress of science and technology while preventing misuse of high-consequence material. Furthermore, it needs to be considered that such legislation/regulation could affect bioeconomy, for example, very strict regulation in a country might cause a relocation of projects, jobs and funding to other less regulated countries with limited national oversight. To avoid such a situation, measures are needed whereby countries with lax or no regulations would not be considered qualified/trusted to handle high-consequence material.

This subsection 8.1 aims to guide oversight at a national level. A two-tier system is proposed to oversee work with high-consequence material at the regulatory and institutional level. At the regulatory level, a national list of high-consequence material should be established informed by risk assessments, while at the institutional level, institutions identify and address risks associated with high-consequence research (Fig. 8.1). Complete implementation of this two-tier system might not be possible in all countries, but certain elements of it could complement national legislation and regulation on biosafety and laboratory biosecurity.

8.1.1 Hybrid approach to regulate high-consequence material

A hybrid approach with risk- and evidence-based elements (risk-based) and a frequently updated list of pathogens (list-based) could be a feasible solution for a national regulatory framework to address biosafety and laboratory biosecurity. It would consist of a list of pathogens or other high-consequence material that are regulated based on risk assessments at the national level, together with a research review system by the IBCs that functions as a feedback loop to communicate new developments and insights to the national regulatory body. This would trigger the review of an existing risk assessment or the performance of a new risk assessment of the regulated high-consequence material by the national regulatory authority. This approach allows the parties involved to address the risks flexibly at a local level and enhances the ability of the national regulatory authority to react to new developments quickly.

On the regulatory side, the national authority needs to develop a list of regulated high-consequence materials such as pathogens, toxins, nucleic sequences (sequences of concern) and created phenotypes that could be used in or result from high-consequence research. Determining which high-consequence materials require regulation should be based on risk assessments and scientific knowledge that enhanced pathogenicity or other biosecurity-relevant properties pose a serious risk to human, animal and plant health or safety. Enhancement of virulence, transmission, host susceptibility and other key factors caused by genetic and/or microbiological manipulations must be monitored in known pathogens with pandemic potential. Inclusion criteria for phenotypes covered in the regulation could be identified by the high-consequence research decision tree in the biosecurity risk assessment template in Fig. A1.1.

The other part of this hybrid approach is the oversight function of the IBC which could involve evaluation of research projects, periodic review of progress reports, review or undertaking of risk assessments, supervision of the implementation of risk control measures, and screening research articles for biosecurity-relevant content before submission to a scientific journal. The oversight function could also be extended and applied more globally in regional or supra-regional guidance documents and with the development of technical tools assisting oversight and research governance systems. The establishment of an international multistakeholder platform would help such tools and systems work better.

8.1.2 Risk assessment

The risk assessment framework applying the risk- and evidence-based approach used in the laboratory biosafety manual is applicable for different settings and levels, including the two tiers proposed – the national regulators and IBCs. Both tiers must perform and/or review risk assessments for biosafety and/or biosecurity to fulfil their roles and responsibilities in the two-tier system.

Roles and responsibilities at the national level

On the regulatory side, risk assessments need to be performed to identify high-consequence material that should be restricted and/or controlled, and guidance needs to be given to the institutions that work with such material.

The national authority may establish a committee of independent experts on biosafety/biosecurity (for example, a national biosafety committee) to perform the risk assessments and/or regularly review them to identify high-consequence material that needs to be regulated. The committee may also assess which, if any, non-high-consequence material could be transformed into high-consequence material with minor genetic modifications.

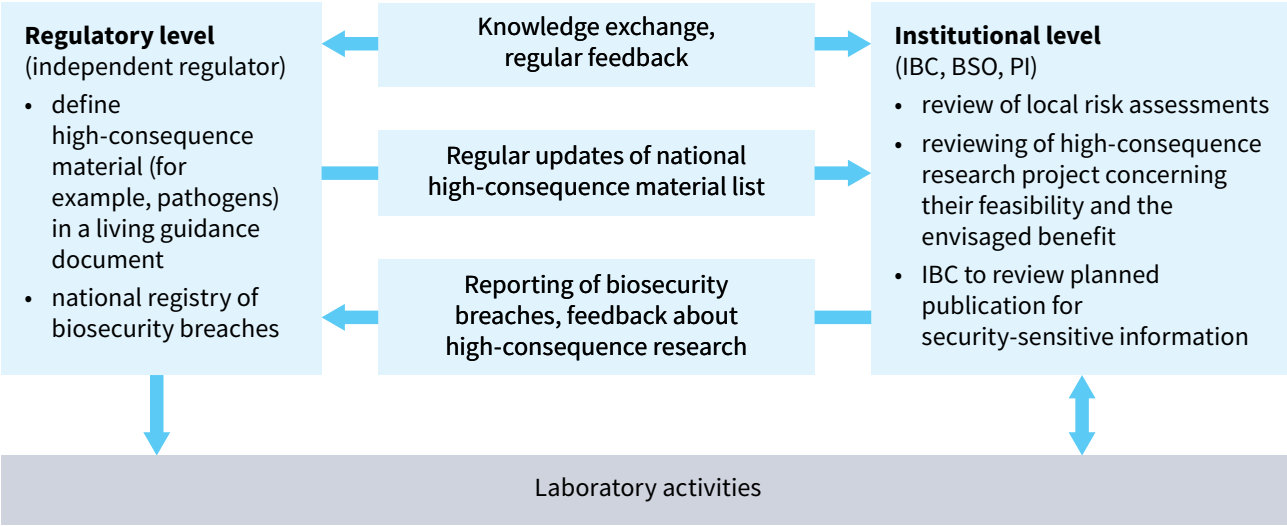

Fig. 8.1. Schematic overview of a two-tier system for national regulation of high-consequence research and material

Based on the risk assessments, the regulatory body needs to list the institutions/laboratories that work with restricted material and provide them with guidance on which areas should be considered in an institutional biosecurity risk assessment for work with restricted high-consequence material – such as physical security, personnel reliability (insider threats), cybersecurity, outsider threats, and high-consequence materials and methods, namely: biological agents; laboratory animals; plants; equipment; techniques; and laboratory procedures and processes (for example, sample taking, transfer/transport and procurement). Additionally, the national authority could support institutions to implement locally relevant and sustainable risk control measures based on the assessed risks by providing funding and strengthening IBCs by defining a central role for them in reviewing and/or performing local risk assessments.

Periodic reviews or audits by the national regulatory authority of the institutions/laboratories possessing, transferring and working with high-consequence material and of the policies and procedures of their IBCs might help sustain and strengthen biosafety and laboratory biosecurity.

Furthermore, the regulatory body needs to ensure that the personnel involved in risk assessments in both tiers have the required expertise and training, and can provide measures for awareness-raising for laboratory biosecurity.

Agreements, such as the Australia Group list, could be applicable to control the export of listed toxins (and toxin subunits), pathogens and their genetic material.

Roles and responsibilities at the institutional level

The IBCs need to perform and/or review the local risk assessments of work with restricted high-consequence material and ensure that any legal requirements are complied with. As well as the roles and responsibilities listed in subsection 4.2 Institutional biosafety committee, the IBC may also need to:

- perform an overarching risk assessment of high-consequence research that spans all the institutional work with restricted high-consequence material;
- supervise the implementation of locally relevant and sustainable risk control measures;

- set a period for reviewing or triggering the reviewing of existing risk assessments in case of changes, new developments, or information or instructions from the national authority; and
- report findings of high-consequence research and/or on high-consequence material to the regulatory authority (feedback loop).

8.1.3 Gain-of-function experiments and high-consequence research

Biosafety and laboratory biosecurity legislation/regulation are aimed particularly at gain-of-function experiments and other high-consequence research in order to oversee laboratory activities that could have severe or even catastrophic consequences for human life if deliberately misused or if high-consequence material were inadvertently released. Society may be critical of these types of experiments; therefore, public perception must be taken into account when establishing the legislation/regulation. Transparency, open dialogue and clearly defined roles and responsibilities of the national regulatory bodies and the IBCs could help to address public concern about and mistrust of high-consequence research. The two-tier system with the national regulatory authority and the IBCs ensuring properly conducted risk assessments and implementation of risk control measures to safeguard laboratory activities provides a balanced approach that does not hinder beneficial high-consequence research, including gain-of-function research. Furthermore, the two-tier system strengthens the IBCs in their role of reviewing laboratory activities involving high-consequence materials.

Roles and responsibilities at the national level

A national regulator, ideally independent from other national authorities, should develop a living guidance document based on the risk- and evidence-based approach for biosafety and laboratory biosecurity that outlines inclusion criteria for biosecurity-relevant material for which possession and handling would need restriction. This document should be regularly reviewed and revised when new information or developments arise, for example, from the feedback loop from the IBCs or scientific publications. It could include characteristics of the high-consequence material and experiments and/or the expected outcome of the planned research work. Finding one of these inclusion criteria in the institutional work would trigger a review of the research project by the IBC with reporting back to the national authority. The national regulatory framework would retain information on institutions/laboratories and principal investigators conducting high-consequence research and have a system that enables independent governmental inspections to ensure that this work is done as safely and securely as possible.

Roles and responsibilities at the institutional level

Determining and evaluating high-consequence research at the institutional level so as to address biosecurity and biosafety risks of the proposed/on-going research rely on cooperation between the IBC and the principal investigator. The responsibilities of the IBC include the following activities.

- Conduct or review biosafety and biosecurity risk assessments and supervise the implementation of risk control measures.
- Identify and address gain-of-function aspects that the principal investigator might not realize, based on inclusion criteria set up by the national regulator or its list (see Annex 1).
- Evaluate the feasibility of planned studies to avoid permitting research that has risk but is unlikely to accomplish the desired result.

- Evaluate the benefits of the high-consequence research (for the population, the environment) in relation to the assessed risk. Recommend changes to the research plan if there is doubt that the expected benefits of this research can be achieved.
- Develop strategies to address unexpected gain-of-function or high-consequence research during an ongoing research project.
- Based on a comprehensive evaluation, decide, together with the funder and in consultation with the principal investigator, if experiments should be performed or not.
- Consider the involvement of other stakeholders such as the government or the community in the decision to allow experiments to be performed or not.
- Ensure that biosafety and biosecurity risk control measures are implemented, if it has been decided to allow the research project to go ahead.
- Ensure that the experiments are conducted transparently and that the research process is documented.
- Report to and/or communicate with the regulatory authority (feedback loop) regarding new developments, insights, findings and/or information about the high-consequence research/material .

8.1.4 Possession, creation and sharing of high-consequence material

WHO advocates an open-sharing policy for genomic data of pathogens and biological material, and many other initiatives and institutes support WHO's call and joined efforts to encourage open sharing . While these activities aim to promote science and progress in the treatment of diseases, there are biosafety and laboratory biosecurity risks in sharing high-consequence material that need to be addressed.

The composition or form of the high-consequence material – such as a living organism, inactivated material, isolated DNA (genome or smaller molecules), genomic library, DNA sequence information or synthesized DNA – should be considered when determining the risk of handling it and this may affect restrictions for import, export or possession.

Furthermore, the people/body with whom the high-consequence material will be shared (for example, cooperation partner, other states) and what conditions and requirements will apply need to be evaluated.

Roles and responsibilities at the national level

A national authority regulates the possession of high-consequence material through the national regulatory programme which holds the relevant information (for example, in form of a register) on institutions/laboratories and, if feasible, principal investigators working with these materials. The regulatory body needs to define rules for the sharing of high-consequence material at a national level and with institutions in other countries. These rules could include certain requirements (for example, appropriate laboratory equipment, performance of risk assessments) and duties (for example, reporting of biosafety and biosecurity incidents) for institutions working with or handling high-consequence material.

Roles and responsibilities at the institutional level

An IBC needs to have systems in place to keep track of the high-consequence material stored, handled and shipped at its institution. Furthermore, the creation of phenotypes that meet the criteria for high-consequence research/material (see Annex 1) from non-regulated biological

agents during the course of the research needs to be overseen and reviewed regularly. The IBC also needs to undertake regular checks to ensure that the requirements set up by the national regulatory body for working with high-consequence material are being followed. If biosafety and biosecurity incidents happen at the institution, the IBC should oversee and review reporting from the principal investigator to the national authority (or any other organization if necessary) and follow up on corrective measures. The IBC needs to review material transfer agreements that describe in detail the requirements for receiving and transferring high-consequence material.

8.1.5 National inventory of high-consequence material and biosecurity-relevant equipment

To meet international agreements and keep track of high-consequence material present in a country's laboratories, the national authority should establish a national inventory of high-consequence material, which should include biosecurity-relevant equipment such as DNA synthesizers. The national authority should also ensure oversight of institutions in terms of material stored and handled.

As part of the hybrid approach, a current list of existing regulated high-consequence material and biosecurity-relevant equipment, defined by risk assessments, must be maintained at both the national and institutional levels.

Roles and responsibilities at the national level

The regulatory body needs to maintain and update a register of restricted high-consequence material and biosecurity-relevant equipment informed by risk assessments. Review of the register could be triggered after a defined period or when new information becomes available, for example, feedback from the IBC or from scientific articles. The national authority also needs to take the following actions.

- Establish a register of institutions with listed high-consequence material (the type of material not the amount) and biosecurity-relevant equipment.
- Provide electronic means (such as a database) for registered institutions to update and modify information on high-consequence material and biosecurity-relevant equipment.
- Provide oversight of the institutions (such as reporting requirements and inspections).
- Define and regulate biosecurity-relevant equipment.
- Oversee projects where biosecurity-relevant equipment is used (such as requiring the IBC to report activities with this equipment or keep track of the output).
- Establish requirements for storage and handling of different types of high-consequence material (for example, DNA and living organisms).
- Introduce a system that enables institutions to qualify for registration as an establishment to handle or store high-consequence material and biosecurity-relevant equipment.
- Provide guidance to institutions that decide to stop conducting research on restricted material on de-registering and destroying high-consequence material, and oversee the process.
- Provide guidance and support to IBCs.
- Provide funding for risk control measures for handling high-consequence material.

Roles and responsibilities at the institutional level

The commitment and active participation of the IBC is crucial for the establishment and maintenance of the national inventory in relation to: registration of the institute; feedback to the national regulatory authority on local risk assessment outcomes; reporting of material stored, moved and handled; support of inspections; and provision of updates on research projects with high-consequence material and other biosecurity-relevant equipment.

The IBC needs to develop institutional policies in line with the requirements set up by the national regulatory body, support the principal investigator in applying for funding to implement the necessary risk control measures, implement cybersecurity risk control measures to ensure secure access to the national inventory database, and conduct or review local risk assessments and report any new information to the national regulatory authority.

8.2 International framework for biological risk legislation

The United Nations Office for Disarmament Affairs (UNODA) backs multilateral efforts to reduce global armament with the ultimate goal of complete disarmament. UNODA supports the Committee (United Nations Disarmament Commission) established in line with Security Council Resolution 1540 (2004) *(44)*. In this resolution, the Security Council stated that "all States shall refrain from providing any form of support to non-State actors that may attempt to develop, acquire, manufacture, possess, transport, transfer or use nuclear, chemical or biological weapons and their means of delivery, in particular for terrorist purposes"

UN Member States are obliged to prepare and implement proper legislative measures to prevent proliferation of such weapons and delivery to non-State actors (that is, persons or groups acting outside of an official government authority).

UNODA focus areas include:

- facilitating regional cooperation to enable national implementation activities,
- enabling cooperation between international, regional and subregional organizations,
- promoting effective partnerships between key stakeholders including civil society, private sector and academia, and
- managing the activities of the UN Trust Fund for Global and Regional Disarmament.

8.2.1 United nations Secretary-General's Mechanism for Investigation of Alleged Use of Chemical and Biological Weapons

The UN Secretary-General's Mechanism for Investigation of Alleged Use of Chemical and Biological Weapons is a resource of the UN Secretary-General to examine alleged uses of chemical and biological weapons reported by Member States. UNODA oversees the Mechanism. To investigate reported suspicions, the UN Secretary-General is supported by qualified experts, consultants and analytical laboratories that are provided by the Member States *(44)*.

8.2.2 Biological Weapons Convention

The Biological Weapons Convention *(45)* effectively prohibits the development, production, acquisition, transfer, stockpiling and use of biological and toxin weapons. It is the first multilateral disarmament treaty banning an entire category of weapons of mass destruction. It entered into force on 26 March 1975. The Biological Weapons Convention currently has 185

States Parties and four Signatory States. States Parties to the Convention agree, "never in any circumstances to develop, produce, stockpile or otherwise acquire or retain: (1) microbial or other biological agents, or toxins whatever their origin or method of production, of types and in quantities that have no justification for prophylactic, protective or otherwise peaceful purpose; and (2) weapons, equipment or means of delivery designed to use such agents or toxins for hostile purposes or in armed conflict". The Biological Weapons Convention has 15 articles. Over the years, it has been supplemented by a series of additional understandings reached at subsequent review conferences. The Convention is a key element in the international community's efforts to address proliferation of weapons of mass destruction and it has established a strong awareness against biological weapons.

In 1987, States Parties to the Convention introduced confidence building measures *(45)*. Their objectives are to improve international cooperation in peaceful biological activities, prevent or reduce the occurrence of ambiguities, and alleviate doubts and suspicions about the development of biological weapons. The confidence building measures consist of the following six measures:

- exchange of information on: (i) research centres and laboratories, and (ii) national biological defence research and development programs;
- exchange of information on outbreaks of infectious diseases and similar occurrences caused by toxins;
- encouragement of the publication of results and promotion of the use of knowledge gained;
- declaration of legislation, regulations and other measures;
- declaration of past activities in offensive and/or defensive biological research and development programmes; and
- declaration of vaccine production facilities.

The States Parties submit national reports on confidence building measures annually to the implementation support unit of the Biological Weapons Convention. The Convention does not have a mandate for verification of information in the reports or inspections of facilities in the country. An electronic platform for confidence building measures was established in 2018, which enables the online submission of reports. The questionnaires of confidence building measures are collected through the national focal points (for example, national authorities).

8.2.3 International health regulations (2005)

The IHR (2005) is a legally binding agreement among 196 countries, including all WHO Member States, to build the capability to detect, report and respond to potential public health emergencies worldwide *(3)*. The IHR (2005) were adopted by the 58th World Health Assembly in May 2007 and entered into force on 15 June 2007. With international trade and travel expanding globally, the risk of greater spread of infectious diseases is increasing. There is a growing need to address the emergence or re-emergence of pathogens and other public health risks at a global level. The main objective of the IHR (2005) is, "to prevent, protect against, control and provide a public health response to the international spread of disease in ways that are commensurate with and restricted to public health risks, and which avoid unnecessary interference with international traffic and trade." The IHR (2005) requires all WHO Member States to have the following core capacities:

- surveillance to detect potential threats,

- reporting systems to provide notifications on specific diseases and any potential international public health emergencies,
- capability to respond to public health threats, and
- collaboration with other countries to make decisions during public health emergencies.

The States Parties must notify WHO of any event that may represent a public health emergency of international concern based on defined criteria. Designated national IHR focal points act as links between States Parties and WHO. To ensure implementation of the IHR (2005) by Member States, an IHR monitoring and evaluation framework was developed by WHO. This framework includes four processes, the following two of which examine biosafety and biosecurity.

- The States Parties Self-Assessment Annual Reporting assesses the extent to which biosafety and biosecurity measures have been implemented in a country *(4)*.
- The Joint External Evaluations measures the functioning of a national framework for biosafety and biosecurity and related mechanisms *(5)*. Biosafety and biosecurity are one of the 19 technical areas evaluated in Joint External Evaluations. The national biosafety and biosecurity framework needs to consider training and practices in human, animal and agricultural facilities, especially in facilities handling/storing high-consequence agents. These facilities should be identified and monitored and their physical security, information security, transportation security, personnel security are evaluated using a specific tool. The Joint External Evaluations recommends limiting the number of facilities housing high-consequence agents.

Under the IHR (2005), the States Parties Self-Assessment Annual Reporting is mandatory and Joint External Evaluations are voluntary. The two other processes – after-action reviews and simulation exercises – are also voluntary.

8.2.4 Cartagena Protocol on Biosafety

This protocol has been in effect since 11 September 2003 *(47)*; 103 countries are signatories. It complements the Convention on Biological Diversity and addresses the risks related to modern biotechnology which have led to living modified organisms and genetically modified organisms, and the need for safety, precautions and balance between economic benefits and public health *(46)*.

8.2.5 Multilateral export control regimes

A multilateral export control regime is a group of countries that support the non-proliferation of weapons of mass destruction. Even though not legally binding, countries involved in multilateral export control regimes should them implemented through supranational and/or national legislation.

For biological high-consequence material, the Australia group *(16)* and the Wassenaar Agreement *(48)* are relevant. The Australia Group has 42 participating countries plus the European Union which apply export control of listed biological (and chemical) material that could be misused as biological (and chemical) weapons. The Wassenaar arrangement has 42 participating states and includes a list of restricted technologies including dual-use goods and technologies. Items on the list must be controlled by another regime, such as the Australia group.

8.2.6 Guidance documents

The W*HO guidance on implementing regulatory requirements for biosafety and biosecurity in biomedical laboratories – a stepwise approach (49)* outlines how to implement regulatory requirements for biosafety and biosecurity at a national level. It provides a stepwise approach for developing a regulatory framework that promotes the implementation and improvement of biosafety and biosecurity measures in biomedical laboratories.

The World Organisation for Animal Health's *Manual of diagnostic tests and vaccines for terrestrial animals (50)* includes a section on biosafety and biosecurity in managing biological risk in veterinary laboratories and animal facilities. This manual provides guidance on laboratory activities undertaken in veterinary laboratories and animal facilities based on a risk- and evidence-based approach.

An efficient and practical approach to biosecurity published by the Centre for Biosecurity and Biopreparedness describes the implementation of biosecurity laws and establishment of national and regional infrastructures to address biosecurity risks *(51)*. As well as the necessary steps, it gives practical advice on how to establish a robust national biosecurity system.

The *Biosafety in microbiological and biomedical laboratories (BMBL) (42)*, developed by the United States Centers for Disease Control and Prevention and the National Institutes of Health, is a comprehensive resource for best practices in biosafety and biosecurity in laboratory settings. The sixth edition provides advice on biosecurity, including risk assessment strategies and guidance on developing a laboratory biosecurity programme.

9 References

1. Biorisk management: laboratory biosecurity guidance, first edition. Geneva: World Health Organization; 2006 (**https://iris.who.int/handle/10665/69390**, accessed 1 February 2024).
2. Laboratory biosafety manual, fourth edition. Geneva: World Health Organization; 2020 (Laboratory biosafety manual, fourth edition and associated monographs) (**https://iris.who.int/handle/10665/337956**, accessed 1 February 2024).
3. International Health Regulations (2005), third edition. Geneva: World Health Organization; 2008 (**https://iris.who.int/handle/10665/43883**, accessed 1 February 2024).
4. International Health Regulations (2005): state party self-assessment annual reporting tool, second edition. Geneva: World Health Organization; 2021 (**https://iris.who.int/handle/10665/350218**, accessed 1 February 2024).
5. Joint external evaluation tool: International Health Regulations (2005), third edition. Geneva: World Health Organization; 2022 (**https://iris.who.int/handle/10665/357087**, accessed 1 February 2024).
6. A74/18. Enhancement of laboratory biosafety. Geneva: World Health Organization; 2021 (**https://iris.who.int/handle/10665/358263**, accessed 1 February 2024).
7. Global guidance framework for the responsible use of the life sciences: mitigating biorisks and governing dual-use research. Geneva: World Health Organization; 2022. (**https://iris.who.int/handle/10665/362313**, accessed 1 February 2024).
8. West RM, Gronvall GK. CRISPR cautions: biosecurity implications of gene editing. Perspect Biol Med. 2020;63(1):73–92. https://doi.org/10.1353/pbm.2020.0006
9. Trump BD, Florin M-V, Perkins E, Linkov I, editors. Emerging threats of synthetic biology and biotechnology: addressing security and resilience issues, first edition. Dordrecht: Springer; 2021. **https://doi.org/10.1007/978-94-024-2086-9**
10. Bier E. Gene drives gaining speed. Nat Rev Genet. 2022; 23(1):5–22. https://doi.org/10.1038/s41576-021-00386-0
11. Pugh J. Driven to extinction? The ethics of eradicating mosquitoes with gene-drive technologies. J Med Ethics. 2016;42(9):578–81. https://doi.org/10.1136/medethics-2016-103462
12. Cole J, Morris P, Dickman MJ, Dockrell DH. The therapeutic potential of epigenetic manipulation during infectious diseases. Pharmacol Ther. 2016;167:85–99. https://doi.org/10.1016/j.pharmthera.2016.07.013
13. Paschos K, Allday MJ. Epigenetic reprogramming of host genes in viral and microbial pathogenesis. Trends Microbiol. 2010;18(10):439–47.
14. Gómez-Tatay L, Hernández-Andreu JM. Biosafety and biosecurity in synthetic biology: a review. Crit Rev Environ Sci Technol. 2019;49(17):1587–621. https://doi.org/10.1080/10643389.2019.1579628
15. Ahteensuu M. Synthetic biology, genome editing, and the risk of bioterrorism. Sci Eng Ethics. 2017;23(6):1541–61. https://doi.org/10.1007/s11948-016-9868-9
16. Australia Group common control list handbook volume II: biological weapons-related common control lists. Washington, DC: United States Government; 2021 (**https://www.dfat.gov.au/sites/default/files/australia-group-common-control-list-handbook-volume-ii.pdf**, accessed 1 February 2024).
17. International Gene Synthesis Consortium; 2017 (**https://genesynthesisconsortium.org/**, accessed 6 October 2021).
18. Fabio Urbina, Filippa Lentzos, Cédric Invernizzi, Sean Ekins. Dual use of artificial-intelligence-powered drug discovery: Comment. Nature Machine Intelligence 2022; (4):189–91.
19. O'Brien JT, Nelson C. Assessing the Risks Posed by the Convergence of Artificial Intelligence and Biotechnology. Health Secur 2020; 18(3):219–27.
20. WHO. Ethics and governance of artificial intelligence for health. World Health Organization 2021 Jun 28 (**https://www.who.int/publications/i/item/9789240029200**, accessed 26 May 2023).
21. Keulartz J, van den Belt H. DIY-bio-economic, epistemological and ethical implications and ambivalences. Life Sci Soc Policy. 2016;12(1):7.
22. Landrain T, Meyer M, Perez AM, Sussan R. Do-it-yourself biology: challenges and promises for an open science and technology movement. Syst Synth Biol. 2013;7(3):115–26. **https://doi.org/10.1007/s11693-013-9116-4**
23. An institution for the do-it-yourself biologist [website]. DIYbio; 2023 (**https://diybio.org/**, accessed 30 March 2023).

24. Bernard R, Bowsher G, Sullivan R, Gibson-Fall F. Disinformation and epidemics: anticipating the next phase of biowarfare. Health Secur. 2021;19(1):3–12.
25. Dual use life science research ("DUR/C"): dialogue with science editors and publishers. Meeting report 28 July 2020. Geneva: World Health Organization; 2020 (**https://iris.who.int/handle/10665/350963**, accessed 1 February 2024).
26. Dual use – dual use potential of life sciences research [internet]. Berlin: Robert Koch Institute; 2023 (**https://www.rki.de/EN/Content/infections/Dual_Use/code_of_conduct.html**, accessed 30 March 2023).
27. Biosafety programme management. Geneva: World Health Organization; 2020 (Laboratory biosafety manual, fourth edition and associated monographs) (**https://apps.who.int/iris/handle/10665/337963**, accessed 1 February 2024).
28. Risk assessment. Geneva: World Health Organization; 2020 (Laboratory biosafety manual, fourth edition and associated monographs) (**https://iris.who.int/handle/10665/337966**, accessed 1 February 2024).
29. The Tianjin Biosecurity Guidelines for Codes of Conduct for Scientists [internet]. Tianjin University Center for Biosafety Research and Strategy, Johns Hopkins Center for Health Security and the Interacademy Partnership; 2021 (**https://www.interacademies.org/sites/default/files/2021-07/Tianjin-Biosecurity-Guidelines-Codes-Conduct.pdf**, accessed 1 February 2024).
30. Decontamination and waste management. Geneva: World Health Organization; 2020 (Laboratory biosafety manual, fourth edition and associated monographs) (**https://iris.who.int/handle/10665/337958**, accessed 1 February 2024).
31. Crawford E, Bobrow A, Sun L, Joshi S, Vijayan V, Blacksell S et al. Cyberbiosecurity in high-containment laboratories. Front Bioeng Biotechnol. 2023;11:1240281. doi: 10.3389/fbioe.2023.1240281
32. Creating a password [internet]. National Cybersecurity Alliance; 2020 (**https://www.cisa.gov/sites/default/files/publications/NCSAM_CreatingPasswords_2020.pdf**, accessed 1 February 2024).
33. United Nations Economic Commission for Europe. Agreement concerning the international carriage of dangerous goods by road (ADR): applicable as from 1 January 2023. New York, NY: United Nations; 2022 (**https://doi.org/10.18356/9789210014328**, accessed 1 February 2024).
34. Convention concerning international carriage by rail (COTIF) Appendix C – Regulations concerning the international carriage of dangerous goods by rail (RID). Bern: Intergovernmental Organisation for International Carriage by Rail; 2023 (**https://otif.org/fileadmin/new/3-Reference-Text/3B-RID/RID_2023_e_23_January_2023.pdf**, accessed 1 February 2024).
35. IMDG code. International maritime dangerous goods code (inc. Amendment 41-22), 2022 edition. London: International Maritime Organization; 2022 (**https://www.imo.org/en/publications/Pages/IMDG%20Code.aspx**, accessed 1 February 2024).
36. Technical instructions for the safe transport of dangerous goods by air (Doc 9284), 2021–2022 edition. Montreal: International Civil Aviation Organization; 2022 (**https://www.icao.int/publications/pages/publication.aspx?docnum=9284**, accessed 28 June 2023).
37. Technical instructions for the safe transport of dangerous goods by air (Doc 9284), 2023–2024 edition. Montreal: International Civil Aviation Organization; 2023.
38. Guidance on regulations for the transport of infectious substances, 2023–2024: applicable as from 1 October 2023. World Health Organization; 2024 (**https://iris.who.int/handle/10665/376214**), accessed 23 March 2024).
39. United Nations Economic Commission for Europe. Recommendations on the transport of dangerous goods: model regulations, 21st revised edition (ST/SG/AC.10/1/Rev.21 (Vol.I)). New York, NY: United Nations; 2019. **https://doi.org/10.18356/7c03b465-en**
40. WHO infectious substances shipping training (e-ISST). Geneva: World Health Organization; 2023 (**https://extranet.who.int/hslp/training/course/index.php?categoryid=43**, accessed 30 March 2023).
41. WHO BioHub System: Standard material transfer agreement 1&2 [pilot testing phase]. Geneva: World Health Organization; 2022 (**https://cdn.who.int/media/docs/default-source/campaigns-and-initiatives/biohub/smta_2june2022.pdf?sfvrsn=8fd04f93_1**, accessed 30 March 2023).
42. Biosafety in microbiological and biomedical laboratories (BMBL), sixth edition. Washington, DC: United States Department of Health and Human Services; 2020 (**https://www.cdc.gov/labs/pdf/SF__19_308133-A_BMBL6_00-BOOK-WEB-final-3.pdf**, accessed 30 March 2023).

43. Canadian biosafety standard for facilities handling and storing human and terrestrial animal pathogens and toxins, third edition. Ottawa: Public Health Agency of Canada; 2022 (**https://www.canada.ca/content/dam/phac-aspc/migration/cbsg-nldcb/cbs-ncb/assets/pdf/canadian-biosafety-standard-third-edition.pdf**, accessed 1 February 2024).

44. United Nations Office for Disarmament. Secretary-General's mechanism for investigation of alleged use of chemical and biological weapons (UNSGM) (internet). New York, NY: United Nations; 2023 (**https://www.un.org/disarmament/wmd/secretary-general-mechanism**, accessed 31 March 2023).

45. United Nations Office for Disarmament. Biological Weapons Convention (internet). New York, NY: United Nations; 2021 (**https://www.un.org/disarmament/biological-weapons/**, accessed 7 October 2021).

46. United Nations Office in Geneva. Electronic confidence building measures portal [internet]. United Nations; 2023 (**https://bwc-ecbm.unog.ch/**, accessed 31 March 2023).

47. Cartagena Protocol on Biosafety to the Convention on Biological Diversity [internet]. Montreal: Secretariat of the Convention on Biological Diversity; 2021 (**https://www.cbd.int/doc/legal/cartagena-protocol-en.pdf**, accessed 7 October 2021).

48. Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies. Vienna: Wassenaar Arrangement Secretariat; 2017 (**https://www.wassenaar.org/app/uploads/2018/01/WA-DOC-17-PUB-006-Public-Docs-Vol.II-2017-List-of-DU-Goods-and-Technologies-and-Munitions-List.pdf**, accessed 1 February 2024).

49. WHO guidance on implementing regulatory requirements for biosafety and biosecurity in biomedical laboratories: a stepwise approach. Geneva: World Health Organization; 2020 (**https://iris.who.int/handle/10665/332244**, accessed 1 February 2024).

50. Biosafety and biosecurity: standard for managing biological risk in the veterinary laboratory and animal facilities. In: Manual of diagnostic tests and vaccines for terrestrial animals, twelfth edition. Paris; World Organisation for Animal Health; 2023 (**https://www.woah.org/en/what-we-do/standards/codes-and-manuals/terrestrial-manual-online-access/**, accessed 31 March 2024).

51. An efficient and practical approach to biosecurity. Copenhagen: Centre for Biosecurity and Biopreparedness; 2018 (**https://www.biosecurity.dk/fileadmin/user_upload/PDF_FILER/Biosecurity_book/An_efficient_and_Practical_approach_to_Biosecurity_web1.pdf**, accessed 1 February 2024).

10 Further information

- Culture of biosafety, biosecurity, and responsible conduct in the life sciences. (Self) assessment framework. International Working Group on Strengthening the Culture of Biosafety, Biosecurity, and Responsible Conduct in the Life Sciences; 2020. **https://absa.org/wp-content/uploads/2020/02/Culture_of_Biosafety-Biosecurity_Self-Assessment_Framework.pdf**, accessed 3 February 2024).
- Dual-use quickscan [internet]. Netherlands (Kingdom of the) Biosecurity Office; (**https://dualusequickscan.com/en/**, accessed 3 February 2024).
- Greene D, Brink K, Salm M, Hoffmann C, Evans SW, Palmer MJ. The Biorisk management casebook: insights into contemporary practices. Stanford, CA: Stanford Digital Repository; 2023. (**https://www.nti.org/wp-content/uploads/2023/03/BRM_Casebook_Final.pdf**, accessed 3 February 2024).
- IEGBBR mobile application of biosafety, biosecurity, and dual-use oversight [internet]. International Experts Group of Biosafety and Biosecurity Regulators; 2022 (**https://iegbbr.org/mobileapp.html**, accessed 3 February 2024).

Annex 1. Biosecurity risk assessment template

Prefix

- Has involved personnel filled in a confidentiality declaration?
- Have strategies to lower inherent risks of high-consequence research been applied?
- Are situations given that could facilitate a biosecurity incident?
- Are there any other vulnerabilities that may affect the occurrence a biosecurity incident?

Gather information (identification of hazards, threats and vulnerabilities)

Identification

- Identify high-consequence research and high-consequence material with the flowchart in Fig. A1.1 Should high-consequence research or high-consequence material be identified, a new biosafety risk assessment should be done or an existing biosafety risk assessment for the laboratory should be reviewed additional to the biosecurity risk assessment.

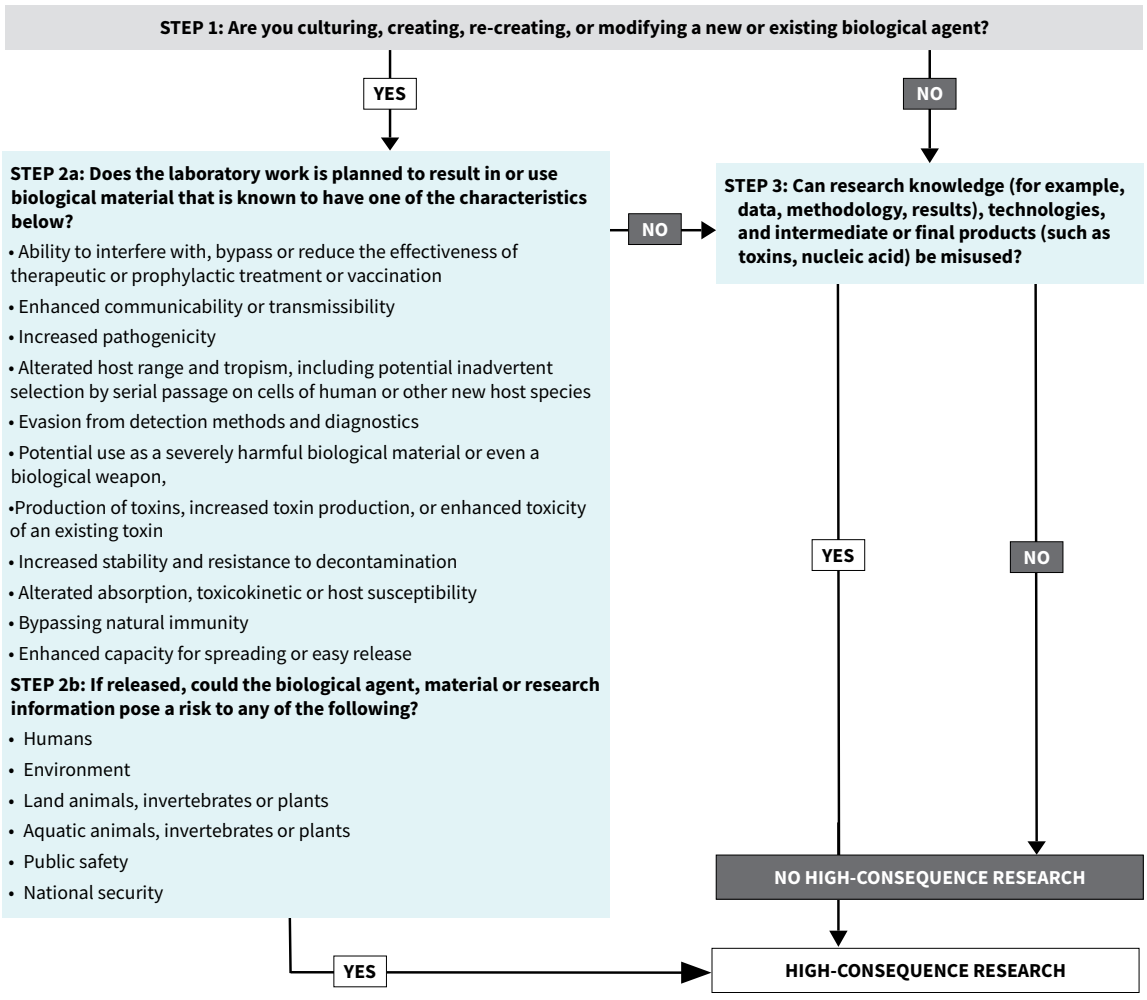

Fig. A1.1. Decision tree for assessing high-consequence research activities

High-consequence material and high-consequence research

- What is the scope of the laboratory work (for example, diagnostics, vaccine production, DNA synthesis, research)?
- What type of work will be conducted with the high-consequence material (for example, diagnostics, propagation, storage, transfer/transport, sample taking, modification)?
- What high-consequence material will be handled and/or stored, and what are their characteristics that are relevant to biosecurity (for example, pathogenicity, and potential misuse)?
- In what form is the high-consequence material in the laboratory (for example, as a low-volume specimen, living biological material) and in what media (for example, in a laboratory animal or as electronic information)?
- What kind of data and information on high-consequence material is handled or stored?
- What kind of biosecurity incident related to the characteristics of the high-consequence material could happen?

Other biological material with biosecurity relevance

- What is the scope of the laboratory work (for example, diagnostics, vaccine production, DNA synthesis, research)?
- What type of work will be conducted with the biological material (for example, diagnostics, propagation, storage, transfer/transport, sample taking, and modification)?
- What biological materials will be handled and/or stored, and what are their characteristics that are relevant to biosecurity (for example, pathogenicity, and potential misuse)?
- In what form is the biological material in the laboratory (for example, low-volume specimen, biological material) and in what media (for example, in a laboratory animal or as electronic information)?
- What kind of data and information on biological material is handled or stored (for example, genetic sequence data)?
- What kind of biosecurity incident related to the characteristics of the biological material could happen?

Personnel security

- What kind of personnel (for example, technical staff, students, and scientists) are involved in the laboratory work? What are their roles and responsibilities? What is their knowledge about the biosecurity aspects and risks of the laboratory work?
- Which types of non-laboratory personnel or external people (for example, facility maintenance workers, visitors or external collaborators) might need to enter a laboratory that has high-consequence material or other biosecurity-relevant material?
- Are there any human factors that may affect biosecurity (for example, work stress, dismissals, disagreements in a team, jealousy, financial debt, drug abuse)?
- Have personnel with access to high-consequence material undergone a background investigation and been considered suitable before being allowed access to the material?
- Are personnel with access subject to periodic or ongoing scrutiny?
- Is there a process for self- and peer-reporting of incidents or behaviours of concern?
- Are there other factors that might affect laboratory biosecurity (for example, legal, cultural, socioeconomic, public perception)?
- What personnel-related biosecurity incident could happen?

Physical security

- In what type of laboratory/facility will the work be performed (for example, conventional laboratory, do-it-yourself laboratory, mobile laboratory)?
- What biosecurity-relevant situations or circumstances could arise if work with, or handling of, biological and/or high-consequence material were undertaken outside the laboratory (for example, sample taking or transfer/transport)?
- Is attendance of personnel in biosecurity-relevant areas of the facility regulated, monitored and/or recorded?
- Is the facility monitored using a video surveillance system or similar? Are there any intruder alarm systems in place?
- How is laboratory access controlled (also to non-laboratory areas such as repositories or sites for decontamination)?
- How does the security clearance process work?
- What kind of biosecurity incident related to physical security could happen?

Inventory security

- What kind of laboratory devices and equipment are used? Essential equipment (for example, refrigerators, freezers, computers or incubators) must also be considered.
- Which biological materials and/or high-consequence materials are included in the inventory list of the facility?
- How is the material accounted for and how often does an inventory audit occur?
- What kind of biosecurity incident related to the inventory could happen?

Information security and cybersecurity

- Which laboratory equipment is connected to the internet or receiving data services?
- What information on the research/work is already publicly available (for example, sequence data on databases)?
- What kind of information is generated, stored or shared about the laboratory work or stored material, and could this information be of biosecurity relevance?
- What kind of biosecurity incident related to information security or cybersecurity could happen?

Society issues

- Do the methods/techniques and/or the material pose any ethical conflict?
- Have there been concerns in the general public about aspects of the laboratory work conducted?
- What kind of biosecurity incident related to society issues could happen?

National/international regulations

- Are national and/or international regulations applied to the laboratory/facilities that affect biosecurity?
- Are there any national/international regulations or recommendations concerning the planned laboratory work?

Evaluate and classify the risks and consequences

Evaluation

- What types of biosecurity incidents could occur (for example, theft, sabotage, destruction of data, deliberate release or diversion of biosecurity-relevant material, espionage, misuse)?
- How could biosecurity incidents occur?
- Where could biosecurity incidents occur?
- Who could create a biosecurity incident?
- What biosecurity incidents could occur in the laboratory, and what could happen during transfer/transport, sample taking or other processes that do not take place in the laboratory (for example, decontamination)?
- What could be the consequences of a biosecurity incident to relevant populations and the extent of the effects? Also consider consequences of biosecurity incidents such as loss of reputation and economic consequences?
- What information or factor influences the consequences the most?
- What is the initial risk (without additional risk control measures) of the laboratory operations (the storage of high-consequence and/or biological material should also be considered as a laboratory operation), sample taking or transfer/transport?
- What is an acceptable risk?
- Are there any circumstances that affect the determination of an acceptable risk?
- Are there any bioethical aspects that need to be considered in the determination of acceptable risk?
- What are the benefits of the intended laboratory work?
- Which risks are unacceptable?
- Can unacceptable risks be controlled, or should the work not proceed?

Classification of consequences - risk

- Negligible - very low risk
- Minor - low risk
- Moderate - medium risk
- Major - high risk
- Serious - very high risk

Classify the initial risk of the laboratory activities before additional risk control measures have been put in place (Table A1.1).

Table A1.1. Classification of risk of the laboratory activities without additional risk control measures

Assessed initial risk	Potential consequences	Actions
☐ Very low	If a biosecurity incident occurred, adverse effects would be negligible.	Undertake the laboratory activity with the existing risk control measures in place.
☐ Low	If a biosecurity incident occurred, there would be minor adverse effects.	Use additional risk control measures if needed.
☐ Medium	If a biosecurity incident occurred, moderate adverse effects would arise that require basic countermeasures or treatment.	Additional risk control measures are advisable.
☐ High	If a biosecurity incident occurred, major adverse effects would arise that would require substantial countermeasures or treatment.	Additional risk control measures need to be implemented before the laboratory activity is undertaken.
☐ Very high	If a biosecurity incident occurred, serious adverse effects would be likely.	Consider alternatives to doing the laboratory activity. Comprehensive risk control measures will need to be implemented to ensure security and national regulations must be adhered to.

Indicate the initial risk of the laboratory activities before additional risk control measures have been put in place and if the risk is acceptable (Table A1.2). Prioritize the implementation of risk control measures.

Table A1.2. Initial risk of each laboratory activity, its acceptability and priority for implementation

Instructions: For additional specification of the risks of individual laboratory activities, determine which risks can/should be reduced and prioritized. For each laboratory activity or procedure of the work assessed, record the initial risks determined from the risk assessment in Table A1.1. Decide whether the work can proceed without additional risk control measures, or whether the risks posed by the work are unacceptable and further risk control measures are needed to reduce these risks. Use the right-hand column of the table below to assign a priority for the implementation of risk control measures based on the identified risks.

Notes.

- When assigning priority, other factors may need to be considered, for example, urgency, feasibility/sustainability of risk control measures, delivery and installation time of these measures, and availability of training.
- To estimate the overall risk, take into consideration the risk ratings for the individual laboratory activities/procedures, separately or collectively as appropriate for the laboratory.

Laboratory activity/ procedure	Initial risk (very low, low, medium, high, very high)	Is the initial risk acceptable? (yes/no)	Priority (high, medium, low)

Determine the overall initial risk.

Overall initial risk	☐ Very low	☐ Low	☐ Medium	☐ High	☐ Very high
Will the work require additional risk control measures?	Yes ☐ No ☐				

Develop a risk control strategy

When developing a risk control strategy, the following factors should be considered.

- What resources are available for risk control measures?
- Are there any recommendations for the work intended from the national authority?
- What risk control strategies are most applicable for the resources available?
- Are resources sufficient to obtain and maintain those risk control measures?
- Are proposed control strategies effective, sustainable and achievable in the local context.

Select and implement risk control measures

When deciding on and implementing risk control measures, the following factors should be considered.

- Is there a system that controls digital/internet access to databases and laboratory equipment?
- Have background checks and personnel reliability screening been performed for personnel?
- Have the personnel been appropriately educated and trained? How is the training status of personnel evaluated and reviewed?
- Have lessons been learnt from previous incidents with biosecurity relevance?
- Are there any risk control measures already in place to mitigate the risks (for example, locked doors, access control systems, a personnel reliability programme)?
- What risk control measures are locally relevant, available and sustainable?
- Are available risk control measures adequately effective, or should multiple risk control measures be combined to enhance effectiveness?
- Is there an auditing system to evaluate the effectiveness of the biosecurity programme and biosecurity risk control measures that have been implemented?
- Do selected risk control measures align with the risk control strategy?
- What is the residual risk after applying risk control measures and is it now acceptable?
- Are additional resources required and available for the implementation of risk control measures?
- Has approval to conduct the work been granted (for example, from the institutional biosafety committee)?
- Have the risk control strategies been communicated to relevant personnel?
- Have necessary items been included in the budget and purchased?
- Are risk control measures incorporated into standard operating procedures?
- Are funding agency rules, regulations and reporting evaluated and implemented?
- Are there any national/international regulations requiring prescribed risk control measures?
- Are the selected risk control measures compliant with national/international regulations?

Describe where and when additional risk control measures are needed, including an assessment of their availability, effectiveness and sustainability (Table A1.3).

Table A1.3. Risk control measures for each laboratory activity, their availability, effectiveness and sustainability and the residual risk

Laboratory activity/ procedure	Selected risk control measure(s)	Residual risk (very low, low, medium, high, very high)	Is the residual risk acceptable? (yes/no)	Are risk control measures available, effective and sustainable? (yes/no)

Classification of consequences/risk

- Negligible/very low
- Minor/low
- Moderate/medium
- Major/high
- Severe/very high

Classify the residual risk that remains after risk control measures have been selected (Table A1.4).

Table A1.4 Classification of residual risk of the laboratory activities after selecting risk control measures

Instructions. Check the residual risk to determine the appropriate actions required.		
Assessed residual risk	**Potential consequences**	**Actions**
☐ Very low	If a biosecurity incident occurred, adverse effects would be very unlikely.	If the identified residual risk is acceptable, no further action is required for laboratory work to proceed.
☐ Low	If a biosecurity incident occurred, the likelihood of adverse effects would be small.	
☐ Medium	If a biosecurity incident occurred, adverse effect would arise that would require basic countermeasures or treatment.	If the identified residual risk is not acceptable, further action is required for the laboratory work to proceed. Re-evaluate your risk control strategy based upon the initial risk of laboratory activities. Actions may include, but are not limited to: • implementing additional risk control measures in accordance with the initial identified risk of laboratory activities to reduce residual risk to an acceptable risk, that is ▪ medium/high initial risk – implement further risk control measures before undertaking the laboratory activity ▪ very high initial risk – implement comprehensive risk control measures before undertaking the laboratory activity to ensure security; • redefining the scope of work such that the risk is acceptable with existing risk control measures in place; • identifying an alternative laboratory with appropriate risk control strategies already in place that is capable of conducting the work as planned.
☐ High	If a biosecurity incident occurred, adverse effects would arise that would require substantial countermeasures or treatment.	
☐ Very high	If a biosecurity incident occurred, catastrophic adverse effects would be likely.	

Determine the overall residual risk.

Overall residual risk	☐ **Very low**	☐ **Low**	☐ **Medium**	☐ **High**	☐ **Very high**
Will work require additional risk control measures?	Yes ☐ No ☐				

The implementation of risk control measures includes:

- communication of incidents, risks and risk control measures,
- purchase/implementation of required risk control measures,
- operational and maintenance procedures, and
- training of personnel.

Review risks and risk control measures

- Have there been any changes in laboratory activities, high-consequence material, personnel, equipment or facilities?
- Is there any new knowledge on high-consequence material and/or biological material being used, laboratory activities and/or personnel?
- Have there been any changes in the determination of an acceptable risk?
- Are there any lessons learnt from incident reports and investigations that may indicate improvements need to be made?
- Has a periodic review cycle been established?
- Has a biosafety risk assessment performed or revised?

Annex 2. Biosecurity emergency response templates

The biosecurity emergency response templates (Table A2.1 to Table A2.6) were developed as a tool for institutions to help plan the emergency response when dealing with high-consequence material and other biosecurity relevant material. The templates need to be customized to local circumstances to ensure a systematic, timely and appropriate response to a biosecurity emergency. The templates can also be used as an aid for training.

Importantly, the institution/organization needs to establish a list of emergency contact numbers and the sequence of alerts. For example, for suspected theft, the alert level may only be the laboratory manager, while for confirmed theft, the institution's senior management may also need to be informed.

Table A2.1. Theft and deliberate or accidental loss of high-consequence material

Step	Response/action
1. Detect (suspect)	• Was the incident detected immediately or belatedly? • Is it the only suspected biosecurity incident? • Was the incident detected by external authorities?
2. Alert	• Notify security personnel and/or external authorities. (**Include telephone number(s)).** • Notify the biosafety officer. (**Include telephone number)** • Notify other relevant personnel (for example, laboratory manager, principal investigator, senior management). (**Include telephone number(s))**
	• Identify the high-consequence material. • Communicate the procedure personnel must follow for theft or loss (deliberate or accidental) that is suspected or confirmed. • Act according to predefined roles and responsibilities of the biosafety officer, security personnel and other relevant personnel.
3. Secure	• Secure/contain the site. • Preserve the scene – avoid touching or moving anything within the scene. • Evaluate or assess the extent of the situation. • Decontaminate if necessary. • Implement measures to prevent further exposure to personnel. • Communicate measures to limit the consequences of theft or loss of the high-consequence material.
4. Investigate	• Collect data (for example, question people present at the time the incident happened, review closed-circuit television). • List high-consequence material samples that are missing. • Cooperate with authorities involved in the investigation.

5. Report, review and improve	• Report to senior/top management and/or the regulatory body. • Review policies and standard operating procedures related to the incident. • Implement lessons learnt.

Table A2.2. Unauthorized/intentional release of high-consequence material

Step	Response/action
1. Detect (suspect)	• Was the incident detected immediately or belatedly? • Is it the only suspected biosecurity incident? • Was the incident detected by external authorities? • What laboratory areas are potentially affected? • What areas outside the laboratory are potentially affected?
2. Alert	• Notify security personnel and/or external authorities. (**Include telephone number(s))** • Notify the biosafety officer. (**Include telephone number)** • Notify other relevant personnel (for example, laboratory manager, principal investigator, senior management). (**Include telephone number(s))** • Specify the high-consequence material and its characteristics that could have been released, and alert personnel, other potentially affected persons and relevant authorities.
3. Secure/evacuate	• Secure/contain the area. • Evacuate the area. • Cooperate with emergency responders and law enforcement agencies to set up containment zones (for example, hot, warm and cold zones). • Triage and decontaminate affected personnel, if necessary. • Describe detailed measures to protect personnel, the community and the environment from the high-consequence material. • Assess measures to limit the consequences of the release of the high-consequence material (first aid, validated method of decontamination).
4. Investigate	• Attempt to identify the biosecurity breach (through, for example, closed-circuit television, personnel interviews, fingerprints). • Preserve the crime scene. • Provide detailed description of the biosecurity breach. • Cooperate with external authorities regarding affected areas outside the laboratory.
5. Report, review and improve	• Report to senior/top management and/or the regulatory body. • Review policies and standard operating procedures related to the incident. • Implement lessons learnt.

Table A2.3. Unauthorized access to laboratory facilities, break-in and intrusion (including vandalism, picketing, occupation, barricade) and violent attacks on personnel

Step	Response/action
1. Detect (suspect)	• Was the incident detected immediately or belatedly? • Is it the only suspected biosecurity incident?
2. Alert	• Notify security personnel and/or external authorities. (**Include telephone number(s))** • Notify the biosafety officer. (**Include telephone number)** • Notify other relevant personnel (for example, laboratory manager). (**Include telephone number(s))** • Warn the laboratory personnel. • Specify the type of unauthorized access (for example, break-in, follow personnel or use of stolen personnel security pass). • If encountering a perpetrator, avoid direct confrontation, run away and hide in a secure place. Take note of the key features of the perpetrator (for example, height, clothing, accent and other characteristics).
3. Secure	• Describe actions and procedures for the safety and security of the affected personnel. • Describe actions and procedures to secure biosecurity-relevant material, technology and information. • Assess any injuries to personnel and property damage. • Assess any compromise to any containment of high-consequences material.
4. Investigate	• Describe the incident in detail. • Investigate the incident according to the institutional policies and country's legal requirements. • Preserve the crime scene. • Cooperate with authorities involved in the investigation.
5. Report, review and improve	• Report to senior/top management and/or the regulatory body. • Review policies and standard operating procedures related to the incident. • Implement lessons learnt.

Table A2.4. Sabotage of laboratory activities

Step	Response/action
1. Detect (suspect)	• Was the incident detected immediately or belatedly? • Is it the only suspected biosecurity incident?
2. Alert	• Notify security personnel and/or external authorities. (**Include telephone number(s)**) • Notify the biosafety officer. (**Include telephone number**) • Notify other relevant personnel (for example, laboratory manager). (**Include telephone number(s)**)
3. Secure	• Describe actions to secure the safety of personnel. • Describe actions to secure biosecurity-relevant material and information. • Describe actions and procedure to limit the consequences of the sabotage.
4. Investigate	• Preserve the crime scene. • Describe measures to determine the extent and consequences of the sabotage.
5. Report, review and improve	• Report to senior/top management and/or the regulatory body. • Review policies and standard operating procedures related to the incident. • Implement lessons learnt.

Table A2.5. Theft of devices, equipment, consumables or non-toxic and non-infectious biological material

Step	Response/action
1. Detect (suspect)	• Was the incident detected immediately or belatedly? • Is it the only suspected biosecurity incident?
2. Alert	• Notify security personnel and/or external authorities. (**Include telephone number(s)**) • Notify the biosafety officer. (**Include telephone number**) • Notify other relevant personnel (for example, laboratory manager). (**Include telephone number(s)**)
3. Secure	• Describe measures to eliminate any risk to personnel. • Describe measures to limit the consequences of the theft of the device, equipment or consumable. • Immediately change security access such as password, personal identification numbers or lock sets.
4. Investigate	• List missing devices, equipment or consumables. • Preserve crime scene. • Review closed-circuit television footage. • Interview relevant personnel such as laboratory personnel or maintenance personnel. • Work with the institution's information technology experts and law enforcement agencies to establish the extent of the data breach for devices containing information.

5. Report, review and improve	• Report to senior/top management and/or the regulatory body. • Review policies and standard operating procedures related to that incident. • Implement lessons learnt.

Table A2.6. Unauthorized digital access or espionage of biosecurity-relevant information

Step	Response/action
1. Detect (suspect)	• Was the incident detected immediately or belatedly? • Is it the only suspected biosecurity incident?
2. Alert	• Notify the system administrator. (**Include telephone number(s))** • Notify the biosafety officer. (**Include telephone number)** • Notify other relevant personnel (for example, laboratory manager). (**Include telephone number(s))**
3. Secure	• Isolate or disconnect the information technology system from external sources. • Shut down the system.
4. Investigate	• Describe the kind of access to biosecurity-relevant information. • Investigate the incident and analyse how the intruder gained access to the server system.
5. Report, review and improve	• Report to senior/top management and/or the regulatory body. • Review policies and standard operating procedures related to the incident. • Implement lessons learnt.

Annex 3. Examples of national biosecurity laws, regulations, guidelines and policies

The following are examples of national approaches to some of the biosecurity challenges that have been described in this document. WHO does not endorse these specific approaches and notes that countries have addressed the issues covered in this document to varying degrees. National approaches address the kinds of biosecurity risks that now exist and vary in how comprehensive they are. It should be noted that biosecurity risks may become more prevalent and/or serious because of emerging technologies.

Australia

The Biosecurity Act of 2015 provides legal authority for all biosecurity activities in Australia. Two regulations were developed under this act: (i) Biosecurity Regulations 2016, which are administered by the Department of Agriculture; and (ii) Biosecurity (Human Health) Regulations 2016 *(1)*, which are administered by the Department of Health and Aged Care.

Canada

Canada has a comprehensive framework for biosafety and biosecurity and guidance for preventing biosecurity incidents such as its Human Pathogens and Toxins Act *(2)*, biosecurity programme *(3)*, and guidelines on biosecurity risk assessment and biosecurity plans *(4, 5)*.

China

China has the Biosecurity Law of the People's Republic of China, 2020 *(6)*. Article 1 states that the law aims to maintain national security, prevent and respond to biosecurity risks, safeguard people's lives and health, protect biological resources and the environment, promote the beneficial development of biotechnology, promote the creation of a community with a shared future for humankind, and bring about the harmonious coexistence of man and nature. The biosecurity law is broad and applies to the following activities:

- prevention and control of major emergent infectious diseases and outbreaks in animal and plants;
- maintenance of security in biotechnology research development and applications;
- management of biological security in pathogenic microbiology laboratories;
- management of security in human genetic resources and biological resources;
- prevention of encroachment by foreign species and preservation of biodiversity;
- implementation of response measures to microbial drug resistance;
- prevention of bioterrorist attacks and use of defence measures against the threat of biological weapons; and
- implementation of other activities related to biological security.

European Union (EU)

The EU regulates high-consequence materials through EU-wide regulations and national laws. The EU's Dual-use Regulation 2021/821 *(7)* governs the export of certain high-consequence materials, while national laws in EU member states impose additional requirements for the handling and storage of such materials.

India

Guidelines for biosafety and biosecurity cover agriculture, veterinary medicine, human health, laboratory research and technological advances. The Regulations and Guidelines for Recombinant DNA Research & Biocontainment 2017 *(8)* consolidates, modifies and updates earlier guidelines. These current guidelines have regulatory outreach with defined mechanisms that include research, containment/laboratory use, export and import, storage and handling, manufacturing, disposal and emergency procedures.

The *Ethical guidelines for application of artificial intelligence in biomedical research and healthcare* are national guidelines for all stakeholders including innovators, developers, researchers, health care professionals, institutions, sponsors and funding agencies involved in research related to artificial intelligence in biomedical research.

Other relevant legislation and guidelines regulate and strengthen the appropriate and safe practices in biological research and biosafety/biosecurity, including: the Environmental Protection Act 1986 *(10)*; rules on hazardous microorganisms, genetically modified organisms or cells *(11)*; the risk analysis framework *(12)*; guidelines on the establishment of containment facilities *(13)*; and the Weapons of Mass Destruction and Their Delivery Systems (prohibition of unlawful activities) Act 2005 *(14)*. The export control of special chemicals, organisms, materials, equipment and technologies of high-consequence are regulated under the relevant provisions of the Foreign Trade (D&R) Act 1992 *(15)*.

Russian Federation

The Russian Federation has a dual-use regulation system in place to control the export of items that can be used for both civilian and military purposes. The primary legislation governing the export control of dual-use items is the Federal Law on Export Control of 2007. This law sets out the legal framework for the control of exports of dual-use items, including the procedures for obtaining licenses for the export of such items.

Laboratory biosecurity is regulated by the following laws and regulations.

- Federal Law on Sanitary and Epidemiological Well-Being of the Population *(16)*. This law establishes the legal framework to ensure the health and epidemiological well-being of the population, including measures to prevent the spread of infectious diseases in laboratory settings.
- Federal Law on the Prevention of the Spread of Infectious Diseases. This law sets out the measures to be taken to prevent the spread of infectious diseases, including those that can be spread in laboratory settings.
- Federal Law on Protection of the Population and Territories from Emergency Situations of Natural and Technological Character. This law sets out the measures to prevent and respond to emergencies that may arise in laboratory settings *(17)*.

- Regulations on biosafety in handling pathogens of human, animal and plant diseases. This regulation provides guidelines on the handling and storage of pathogenic microorganisms, as well as the construction and operation of laboratory facilities.
- Guidelines on biosecurity in laboratories. This document provides detailed guidance on the implementation of biosafety measures in laboratory settings.
- Technical regulations on the safety of biological products. This regulation sets out the safety requirements for the development, production and use of biological products, including vaccines and diagnostic kits.

In addition to these laws and regulations, there are also specific requirements for laboratory personnel, such as the need for training in biosafety practices, the use of personal protective equipment and the establishment of workflows and protocols for handling and disposing of hazardous materials.

The enforcement of laboratory biosecurity regulations in Russia is overseen by various agencies, including the Federal Service for Surveillance on Consumer Rights Protection and Human Wellbeing, which is responsible for monitoring compliance with biosafety regulations in laboratory settings, and the State Research Centre of Virology and Biotechnology, which is responsible for researching and developing vaccines and other countermeasures against infectious diseases.

United States of America

Many presidential directives, executive orders and federal laws have been enacted to protect the nation's research facilities and ensure that proper biosecurity measures are undertaken. The following briefly summarizes the laws on laboratory biosecurity measures to ensure the protection of critical assets from theft, loss or misuse.

Federal Select Agent Program *(18)*. This programme jointly includes the Centers for Disease Control and Prevention (Division of Select Agents and Toxins) and the Animal and Plant Health Inspection Service (Division of Agricultural Select Agents and Toxins). The programme oversees the possession, use and transfer of selected biological agents and toxins which have the potential to pose a severe threat to human, animal or plant health, or to animal or plant products. The programme enhances the nation's oversight of the safety and security of select agents by:

- developing, implementing and enforcing the select agent regulations,
- maintaining a national database on entities working with select agents and toxins,
- inspecting entities that possess, use or transfer select agents,
- ensuring that all individuals who work with these agents undergo a security risk assessment performed by the Federal Bureau of Investigation/Criminal Justice Information Service,
- providing guidance to regulated entities on achieving compliance with the regulations through the development of guidance documents, and conducting workshops and webinars, and
- investigating any incidents in which non-compliance may have occurred.

Executive Order 13486 – Strengthening Laboratory Biosecurity in the United States, 2009 *(19).* This executive order requires that facilities that possess biological select agents and toxins have appropriate security and personnel assurance practices to protect against the theft, misuse or diversion to unlawful activity of the agents and toxins.

Executive Order 13546 – Optimizing the Security of Biological Select Agents and Toxins in the United States, 2010 *20)*. This executive order requires that all selected biological agents and toxins are appropriately secured with regard to their risk of misuse, theft, loss or accidental release, and that security measures are taken in a coordinated manner that balances their effectiveness with the need to minimize the adverse impact on the legitimate use of biological select agents and toxins. To help ensure that these agents and toxins are secured according to the level of risk, the Secretaries of Health and Human Services and Agriculture designated a subset of agents on the Select Agent List that have the greatest risk of deliberate misuse with the most significant potential for mass casualties or devastating effects to the economy, critical infrastructure or public confidence.

Recommended policy guidance for departmental development of review mechanisms for potential pandemic pathogen care and oversight (P3CO) *(21)*. These recommendations at the institutional level and federal level cover the planning, funding and institutional review of research projects involving pathogens with a pandemic potential.

National Biodefense Strategy and Implementation Plan *(22)*. This plan addresses biosecurity and biosafety, among many other issues related to biodefence.

References – Annex 3

1. Biosecurity (Human Health) Regulation 2016: made under the Biosecurity Act 2015 [internet]. Canberra: Australian Government; 2017 (https://www.legislation.gov.au/Details/F2017C00412, accessed 31 March 2023).
2. Human Pathogens and Toxins Act; 2009 [internet]. Ottawa: Government of Canada; 2009 (https://laws.justice.gc.ca/eng/acts/H-5.67/, accessed 31 March 2023).
3. Biosecurity [internet]. Ottawa: Government of Canada; 2021 (https://www.canada.ca/en/public-health/services/laboratory-biosafety-biosecurity/biosecurity.html, accessed 31 March 2023).
4. Canadian biosafety guideline: conducting a biosecurity risk assessment [internet]. Ottawa: Government of Canada; 2018 (https://www.canada.ca/en/public-health/services/canadian-biosafety-standards-guidelines/guidance/conducting-biosecurity-risk-assessment/document.html, accessed 31 March 2023).
5. Developing a comprehensive biosecurity plan [internet]. Ottawa: Government of Canada; 2016 (https://www.canada.ca/en/public-health/services/canadian-biosafety-standards-guidelines/guidance/developing-comprehensive-biosecurity-plan-overview.html, accessed 31 March 2023).
6. Biosecurity Law of the People's Republic of China [internet]. UNEP Law and Environment Assistance Platform; 2021 (https://lawinfochina.com/display.aspx?lib=law&id=33962&EncodingName=big5, accessed 31 March 2023).
7. Dual-use export controls [internet]. Brussels: EUR-Lex; 2021 (https://eur-lex.europa.eu/EN/legal-content/summary/dual-use-export-controls.html, accessed 31 March 2023).
8. Regulations and Guidelines for Recombinant DNA Research & Biocontainment 2017. New Delhi: Government of India; 2017 (https://dbtindia.gov.in/sites/default/files/uploadfiles/Regulations_%26_Guidelines_for_Reocminant_DNA_Research_and_Biocontainment%2C2017.pdf, accessed 31 March 2023).
9. Ethical guidelines for application of artificial intelligence in biomedical research and healthcare. New Delhi: Indian Council of Medical Research; 2023 (https://main.icmr.nic.in/sites/default/files/upload_documents/Ethical_Guidelines_AI_Healthcare_2023.pdf, accessed 31 March 2023).
10. The Environment (Protection) Rules, 1986. New Delhi: Government of India, Ministry of Environment and Forests; 1986 (https://parivesh.nic.in/writereaddata/ENV/THE%20ENVIRONMENT.pdf, accessed 31 March 2023).
11. Rules for manufacture, use, import, export & storage of hazardous microorganisms, genetically modified organisms or cells. New Delhi: Government of India, Ministry of Environment and Forests; 1989 (https://biosafety.icar.gov.in/wp-content/uploads/2015/11/Rules-1989.pdf, accessed 31 March 2023).
12. Risk analysis framework. New Delhi: Government of India; 2016 (https://ibkp.dbtindia.gov.in/DBT_Content_Test/CMS/Guidelines/20181115134923250_Risk_Analysis_Framework.pdf, accessed 31 March 2023).
13. Guidelines for the establishment of containment facilities: biosafety level 2 & 3 and certification of facility, 2020. New Delhi: Government of India; 2020.
14. Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 [internet]. New Delhi: Government of India; 2005 (https://www.indiacode.nic.in/handle/123456789/2017?sam_handle=123456789/1362, accessed 31 March 2023).
15. India's Export Control System. Special chemicals, organism, materials, equipment and technologies (SCOMET). New Delhi: Ministry of Commerce and Industry, Department of Commerce, Directorate General of Foreign Trade; 1992 (https://ibkp.dbtindia.gov.in/DBT_Content_Test/CMS/Guidelines/20181115135754468_Export%20of%20SCOMET%20guidelines.pdf, accessed 31 March 2023).
16. Federal Law No. 52-FZ on Sanitary and Epidemiological Well-Being of the Population. Moscow: Russian Federation; 1999.
17. Federal Law 68-FZ on protection of the population and of the territories from environmental and technological emergencies (https://leap.unep.org/en/countries/ru/national-legislation/federal-law-68-fz-protection-population-and-territories. Moscow: Russian Federation; 1994.
18. Federal Select Agent Program [website]. Atlanta, GA: Centers for Disease Control and Prevention; 2023 (https://www.selectagents.gov/, accessed 31 March 2023).

19. Public Health Emergency. Executive Order 13486 – Strengthening Laboratory Biosecurity in the United States [internet]. Washington, DC: US Department of Health and Human Services; 2023 (**https://www.phe.gov/Preparedness/legal/boards/biosecurity/Pages/default.aspx**, accessed 31 March 2023).

20. Executive Order 13546 – Optimizing the Security of Biological Select Agents and Toxins in the United States [internet]. Washington, DC: The White House; 2010. (**https://obamawhitehouse.archives.gov/the-press-office/executive-order-optimizing-security-biological-select-agents-and-toxins-united-stat**, accessed 31 March 2023).

21. Recommended policy guidance for departmental development of review mechanisms for potential pandemic pathogen care and oversight (P3CO). Washington, DC: US Department of Health and Human Services; 2017 (**https://www.phe.gov/s3/dualuse/documents/p3co-finalguidancestatement.pdf**, accessed 31 March 2023).

22. National biodefense strategy and implementation plan for countering biological threats, enhancing pandemic preparedness, and achieving global health security. Washington, DC: The White House; 2022 (**https://www.whitehouse.gov/wp-content/uploads/2022/10/National-Biodefense-Strategy-and-Implementation-Plan-Final.pdf**, accessed 31 March 2023).

9789240095113

World Health Organization
20 Avenue Appia
CH-1211 Geneva 27
Switzerland

biosafety@who.int