Biosecurity Risk Management in Research

Johannes Rath and Monique Ischi

Contents

Abstract

Despite substantial attention over the last decade, risk management in biosecurity is still fragmented and non-standardized at the operational level. Fragmentation is often a result of selective implementation of various building blocks which all together would constitute a comprehensive biosecurity risk management framework. For example, while most countries have adopted export control measures on biosecurity sensitive materials, additional key elements of such a comprehensive framework, like personnel security and information security, are often not addressed. Furthermore, risk perception varies among stakeholders, and international agreement on the adequate level of risk management (and sometimes even on the need for it) is missing, contributing to the heterogeneity of standards currently applied to biosecurity sensitive research. For example, some countries like the USA have opted for stringent stand-alone biosecurity legislation also covering research, while other countries like Germany operationalize biosecurity primarily through integration in biosafety risk management frameworks. Furthermore, in light of inconsistent, incomplete, and/or missing legal guidance,

J. Rath (✉) · M. Ischi
Department Integrative Zoology, University of Vienna, Vienna, Austria
e-mail: johannes.rath@univie.ac.at

R. Iphofen (ed.), *Handbook of Research Ethics and Scientific Integrity*,
https://doi.org/10.1007/978-3-319-76040-7_10-1

individual and collective responsibility-based risk management frameworks have been proposed by the scientific community. These self-governance attempts by the scientific community have resulted in a plethora of different approaches ranging from simple awareness raising concepts to individual self-censorship of research publications.

This chapter highlights some of the challenges in governing biosecurity sensitive research. Key principles and processes constituting a comprehensive biosecurity risk management framework in line with international risk management standards are outlined and discussed.

Keywords
Risk management · Biosecurity · Dual use · ISO 31000

Introduction

Warren Buffet is attributed to once have said that "Risk comes from not knowing what you're doing." Today mitigating uncertainty has become the key element in risk management with the updated risk management standard ISO 31000:2018 (International Organisation for Standardization 2018) defining risk as "effect of uncertainty on objectives." The evolution of risk management as a stand-alone discipline over the last decades has led to a maturation and consolidation of terms, general concepts, and principles and has been most recently summarized in "Risk Management – Guidelines" issued by the International Standardization Organisation (ISO 31000: 2018). ISO31000 outlines a comprehensive risk management framework building on a structured approach to risk assessment, risk treatment, risk monitoring/review, risk recording/reporting, and risk communication/consultation.

Current Status of Risk Management in Biosecurity Sensitive Research

Although risk management is critical in ensuring and maintaining security overall, biosecurity risk management in research is still in its infancy. The recent failure to proactively address the H5N1 gain-of-function biosecurity controversy was a consequence of inadequate risk management frameworks (Becker 2012). As an example, the attempt by the Dutch government to invoke export control legislation as a means to address existing information security deficiencies in research highlighted the dilemma many countries are in (Enserink 2012). However, systematic personnel security and information security measures for biosecurity sensitive agents and information are rarely implemented today.

Inconsistent country (Arnason 2017) and institutional (Patrone et al. 2012) and individual attitudes in managing biosecurity risks have led to an enigmatic array of approaches. These inconsistencies create loopholes which are highly problematic.

For example, export control legislation is applied to restrict access outside of the EU for technologies and materials and knowledge, which can be used for both civil and military purposes (Aubin and Idiart 2011). Uncovering and analyzing the A. Q. Khan Network (Corera 2009) has shown that such a limited risk management approach solely focussing on export controls is ineffective without effective additional controls that restrict access of dual-use technologies also inside countries.

Critical limitations in risk management of biosecurity sensitive research are:

(a) Lack of Common Terminology

The use of a common terminology is a critical prerequisite for any meaningful risk management approach. Currently, standard definitions are missing. For example, different terms are used to describe similar and often overlapping risks (e.g., dual use, dual-use research of concern (DURC), biorisk), while on the other hand the same term is used to describe unrelated concepts (e.g., the term biosecurity is used to describe control measures in the development and use of bioweapons, while the very same term is also used to describe infectious animal disease control measures).

ISO Guide 73: Risk Management Vocabulary provides a set of generic risk management terms that provide a first step into the development of a standard risk management vocabulary to manage risks in biosecurity sensitive research.

(b) Governance Structures and International Coordination Responsibilities and Accountabilities

Numerous non-binding codes and guidelines have been developed or are under development by and for a variety of stakeholders (Table 1) with varying mandates, objectives, and scope ranging from generic awareness-raising codes of ethics to more detailed practical guidelines.

Depending on the individual code/guideline, the role given to individual or collective self-governance of the scientific community varies. One source of this variation relates to different cultures in governing scientific research. Self-governance of research activities by researchers has a long tradition in certain disciplines like medicine and geographical locations (e.g., the USA), whereas in central Europe, for example, the role of governance by laws is more prevalent, leaving less space for self-governance.

Governing biosecurity risks in research through ethics have also been suggested by including biosecurity into concepts of responsibility and accountability (World Health Organisation 2010). A relevant approach in this context is the systematic inclusion of biosecurity concerns into the Ethics Appraisal Framework of Horizon 2020: (http://ec.europa.eu/research/participants/data/ref/h2020/other/hi/guide_research-misuse_en.pdf). In addition, various countries have opted for legal instruments to govern biosecurity concerns (e.g., US Select Agents Regulation, EU Dual Use Export Control legislation).

The area of biosecurity lacks comparable international coordination such as in the chemical and nuclear area. In contrast to the Chemical Weapons Convention and the Non-Proliferation Treaty, the Biological Weapons Convention (https://www.un.org/disarmament/wmd/bio/), the key international treaty to

Table 1 Examples of codes of conducts in biosecurity and dual use in life sciences

Title	Sponsor	Year	Internet link
Declaration of Washington on biological weapon	World Medical Association, WMA	2003	http://www.wma.net/en/30publications/10policies/b1/index.htm
Europa Bio's Core Ethical Values	The European Association for Bioindustries	2016	https://www.eu/ropabio.org/sites/defaultfiles/Final%20EuropaBio%20Core%20Ethical%20Values%20-%202016%20version.pdf
IUMS Code of Ethics	International Union of Microbiological Societies	2008	https://www.iums.org/index.php/code-of-ethics
Guidelines for researchers on dual use and misuse of research	Working Group Dual Use of the Flemish Interuniversity Council	2017	https://www.uhasselt.be/documents/DOC/2017VLIR003_FolderOnderzoek_EN_DEF_20180212.pdf
IAP Statement on Biosecurity	Inter Academy Panel on International Issues	2005	http://www.interacademies.net/File.aspx?id=5401
Biotechnology, Weapons and Humanity: ICRC outreach to the life science community on preventing hostile use of the life sciences	International Committee of the Red Cross	2004	https://www.icrc.org/eng/assets/files/other/icrc_002_0833.pdf
Tools for the Identification, Assessment, Management, and Responsible Communication of Dual Use Research of Concern	National Institutes of Health	2014	https://www.phe.gov/s3/dualuse/Documents/durc-companion-guide.pdf
A code of conduct for biosecurity	Royal Netherlands Academy of Arts and Sciences	2009	file:///C:/Users/HP/Downloads/20071092.pdf
Biosafety and biosecurity: Standards for Managing Biological Risks in the Veterinary Laboratory	OIE	2015	http://www.oie.int/fileadmin/Home/eng/Health_standards/tahm/1.01.04_BIOSAFETY_BIOSECURITY.pdf
OECD Best Practice Guidelines for Biological Resource Centres	OECD	2007	http://www.oecd.org/sti/emerging-tech/38777417.pdf
Statement on dual-use research of concern and research misuse	BBSRC, MRC and Wellcome Trust position	2014	https://wellcome.ac.uk/sites/default/files/wtp059491.pdf

address biosecurity concerns, is left without a technical organization that carries out international verification and monitoring activities or assists and coordinates international guideline development in biosecurity.

The only widely used document available at the international level is the "Biorisk Management: Laboratory biosecurity" guidance document by the World Health Organisation (2006). Although a respectable attempt in 2006, the document is often generic and with limited conceptual clarity, thereby limiting its practical relevance. For example, in defining the scope, the biosecurity guidance introduces the term "valuable biological material" and provides a definition for it. This definition, however, is far too broad and not coordinated with other guidelines (e.g., in the dual-use context), making it challenging to define perimeters for biosecurity risk management. Furthermore, no comprehensive and structured risk management framework is provided, and individual risk mitigation measures such as information security although helpful are insufficiently detailed to enable an operational application.

Since then the WHO has shifted its focus to an integrated safety-security risk management approach; however, it has provided no further guidance on how such integrated risk management framework could be operationalized (World Health Organisation 2010). Furthermore, an initiative to transform two CWA standards into an ISO standard on biorisk management is still ongoing (International Standardization Organisation 2018). Of note is that this lack in international coordination also hampers agreement on a common terminology as discussed before.

(c) Lack of Conceptual Clarity: Biosecurity versus Biorisk Management
Countries implementing biosecurity legislation and guidance have adopted two different approaches. Some countries like the USA (National Research Council 2010) have issued stand-alone biosecurity legislation, while others like Germany have aimed at integrating biosecurity and biosafety (Bielecka and Mohammadi 2014). Both approaches have pros and cons. However, these inconsistencies make it difficult to develop consistent risk treatment outcomes as scope and objective of the whole risk management process are different.

Toward a Comprehensive Biosecurity Risk Management Framework in Biosecurity Sensitive Research: Principles and Processes

A variety of risk management frameworks exist for various disciplines. ISO 31000:2018 is unique in being a generic, comprehensive, and principle-based framework. As such it is not only suitable to facilitate the integration of biosecurity risk management into the overall risk management framework of an organization but also constitutes a suitable framework for the integration of related objectives like biosafety and public health into one risk management process. Critical pillars in the implementation of ISO31000:2018 compliant risk management frameworks are observation of principles and adherence to a structured risk management process.

Principles

Risk management in ISO 31000:2018 is guided by principles. The following points highlight some of these principles and how they relate to risk management of biosecurity sensitive research.

Value Creation

Security in general is seen as a public good. Enhancing security through risk management of biosecurity sensitive research creates value. However, security is framed in different ways, and whether it is addressed as national, military, civil, or human security has significant impact on the scope of the risk management (Rath et al. 2014), on who the stakeholders are and on what roles they play in the risk management process. Depending on the framing of security, individuals (e.g., researchers), private organizations (e.g., universities, funding institutions, publishers), and public institutions (e.g., export control agencies, police, military, public health institutions) will take on different roles and responsibilities in risk assessment, treatment, monitoring, and communication.

When it comes to value creation, problems arise as these stakeholders often may not share the same value system. For example, medical researchers might be much more willing to define security within the framework of health security, whereas law enforcement might be more familiar with the concept of civil security. This generates challenges in developing a common understanding among stakeholders on how, when, and where risk management of biosecurity sensitive research is a value creating process.

Integral Part of Organizational Processes

In contrast to established risk management frameworks in biological and medical research (e.g., biosafety, ethics), biosecurity is often not well integrated in organizational processes. Critical external stakeholders (e.g., export control authorities, National Advisory Boards like the NSABB, law enforcement agencies, military) act outside established organizational processes (e.g., proposal writing, funding application, conduct of research, publishing, patent application) and structures (e.g., research institutes, funding agencies, publisher, patent office) in research. Decisions by such outside bodies may be inconsistent with internal policies and organizational structures as no common, structured, and consistent risk management framework is applied between internal and external stakeholders. Enhancing risk communication and consultation between internal and external stakeholders (e.g., through expert advisory groups) as well as setting internal organizational structures facilitating communication and consultation (e.g., institutional biosecurity officer/board, ethics, and scientific review committees) would improve the integration of biosecurity into the organizational process of research institutions.

Part of Decision-Making, Timeliness

Organizational processes are often not established that would ensure availability of practical biosecurity risk management expertise (e.g., access to a biosecurity expert)

throughout the whole research cycle. The beginning of a research activity is an especially critical moment for risk management, as at this early stage a large repertoire of risk treatment options, including the option not to do the research, exist. Due to lack of awareness and expertise at research and funding institutions, biosecurity considerations usually do not become part of decision-making. Later recognition of biosecurity concerns in research, e.g., at the publication level, reduces the number of available options (e.g., censorship/publication restriction) to mitigate risks. Timeliness in making biosecurity risk management part of the decision-making process early in the research life cycle would allow for less intrusive and better tailored risk management due to availability of a wider range of risk treatment options. On a practical level, the H5N1 gain-of-function controversy highlighted the need for early engagement in biosecurity preferably at the research conception and funding evaluation stage. The lesson also highlighted the importance of funding institutions as relevant stakeholders and the possibility that through the funding contract legally enforceable safeguards can be introduced.

Based on Best Information Available

Access to security information is restricted, and without such access the level of uncertainty increases substantially making risk management highly challenging. The threat element in biosecurity risk management is far more difficult to assess for individuals (e.g., researchers) outside the security community, and even within the security community, substantial uncertainty often exists on the plausibility of the threat scenario. For example, developing plausible threat scenarios is challenging given the dynamic environment in which, for example, terrorism unfolds. Risk management therefore often focusses on assessing vulnerabilities (e.g., known weaknesses in public health toward certain agents) and mitigating consequences (e.g., vaccinations). Improving access to information (without at the same time compromising security) that would allow researchers to make more realistic threat assessments would improve acceptance and relevance of risk management in biosecurity.

Customized to the Specific Environment

Research is a very unique environment for risk management, and risk treatment needs to take into account the large uncertainties that are inherent to scientific experiments. Managing such uncertainties through an iterative approach by gradually moving from low-risk experiments to higher-risk levels is often recommended.

In addition, customization often becomes challenging as critical risk mitigation measures such as information or personnel security measures are not established at research institutions.

Takes Human and Cultural Factors into Account

Established human and cultural factors in research are challenging when it comes to biosecurity risk management. The openness in which universities address information access, material transfers but also (international) mobility of personnel is challenging and often prohibitive for any attempt to establish information or

personnel security measures. Furthermore, legal frameworks like export control regimes have generic exemption clauses for fundamental or basic research to account for the specific cultural factors in research. From risk management perspective, however, such exemptions limit the available risk treatment options in research, and it is not clear why security risks arising from fundamental research should be handled differently than those arising from applied research or innovation activities.

Dynamic and Responsive to Change

Biosecurity risk management in research in specific needs to be highly dynamic and responsive to change. Two drivers necessitate such a dynamic approach. The first is the specific nature of the threat especially with regard to non-state actors. Threat scenarios involving terrorist and criminal organisations engaging in biological weapons are constantly changing. Second, research itself constantly modifies the risk environment through the creation of new vulnerabilities (e.g., creation of novel pathogenic agents) or the development of new risk treatment approaches (e.g., new prophylactic and treatment options). To account for such innovations, a dynamic and iterative process to risk management is needed.

Systematic

Biosecurity risk management in research has been driven by reactions to crisis, whether it has been the Amerithrax case (McQueen 2014) or the politicizing of the dual-use dilemma in research during the gain-of-function discussion (Hunter 2012; Koblentz and Klotz 2018). Reactionary risk management measures are hardly ever comprehensive and developed in a systematic way but focussed on addressing case-specific shortcomings. Comprehensive risk management frameworks to biosecurity in research that would allow for a systematic approach are still missing.

Structured

In order to ensure consistency and comprehensiveness, biosecurity risk management needs to follow a structured approach that follows a preset logic. ISO 31000:2018 structures the process of risk management into five elements: scope, risk assessment, risk treatment, risk recording and reporting, and risk communication and consultation and risk monitoring and review (Fig. 1). All these elements need to be implemented in a structured biosecurity risk management framework.

Processes

Establishing the Context and Defining Objectives

Context and perimeter definition in biosecurity risk management has been inconsistent and can lead to confusion (Rath et al. 2014). Perimeter risks are often defined very narrowly. For example, framing the H5N1 gain-of-function risks solely as an information security-related risk, with publication restrictions as the critical risk mitigation measure, misses out on other risk mitigation options. In this case, risk management should also have taken into account physical and personnel security

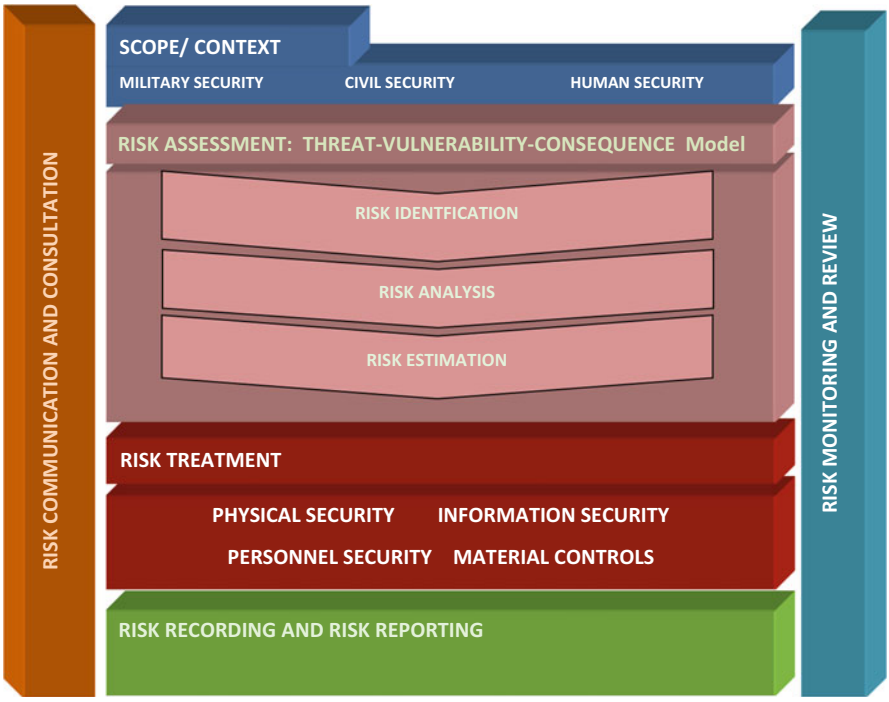

Fig. 1 Comprehensive biosecurity risk management framework based on ISO31000

measures as well as experimental changes like the use of molecular containment systems. Focussing on narrowly defined risk perimeters also provides challenges in developing proportionate risk mitigation measures by acknowledging the interconnectivity of risk management measures taken in biosecurity with areas like public health and biosafety (e.g., information restriction on valuable disease information; see Rath 2014).

Risk Assessment

Within risk assessment the first step called *risk identification* is critical. Biosecurity risks whether located at the threat, vulnerability, or consequence level can only be identified if the relevant knowledge is included into the process. Key stakeholders in biosecurity risk identification are usually the researchers, the research institutions, and the research funding institutions. These actors will have detailed understanding of the proposed research activity. If knowledge in identifying risks from biosecurity sensitive research is missing at the level of these stakeholders, timely biosecurity risk management will not take place. Once risks are identified, risk analysis and risk evaluation should take place to define the level of risk. Both are challenging in the context of biosecurity, due to the already mentioned high levels of uncertainty.

Risk Treatment

Treatment of biosecurity sensitive research risks builds on a variety of treatment options and can focus on personnel security (e.g., security clearance levels), information security (e.g., classification of information), physical security (e.g., effective perimeter control and locked storages), transfer security (e.g., providing access restrictions and controls during material transfers), and material controls (e.g., keeping detailed inventories). Risk avoidance by not starting, continuing, or funding a certain research activity also provides an option and needs to be evaluated against loss of potential benefits. Such benefits from biosecurity sensitive research can be significant, for example, in the areas of public health and biodefence (Selgelid 2016).

Risk Recording and Reporting

Recording and responsible reporting of biosecurity risks in research is challenging. Research is often built on the concept of free knowledge communication, and initiatives to foster the free flow of information (e.g., open access) are actively promoted. Unrestricted reporting of risks and vulnerabilities in security, however, might further increase the risks. Therefore, alternative ways of reporting risks of biosecurity sensitive research should be evaluated (e.g., temporary classification, information access only to individuals holding relevant personnel clearances).

Risk Communication and Consultation

Researchers often tend to exaggerate risks as it may support their research agenda and in the past biosecurity risks have often been communicated through worst-case scenarios. As a consequence, responsible risk communication to the non-expert community (e.g., media, politicians, and lay people) has become a challenge.

Risk consultation, for example, by initiating the inclusion of biosecurity experts into the risk management process in order to improve decision-making is not common and should be further increased. This can be done through the nomination of expert advisors but also by establishing advisory panels and boards.

Risk Monitoring and Review

Finally, continuous monitoring and review of biosecurity risks is usually not foreseen due to the lack of competent monitoring units. Exceptions exist in the areas where biosecurity is integrated into biosafety and adequate biosafety oversight structures have been established or in certain legal contexts. Nonetheless, since biosecurity risks are highly dynamic, routine monitoring to support an iterative approach to risk management is important.

Conclusion

The use of biological agents for malevolent purposes and as a weapon of mass destruction is a serious and real threat in current times. In no other areas of weapons of mass destruction does research play such a dominant role in creating and

managing these risks. Current risk management principles and processes applied to biosecurity sensitive research are inconsistent, unstructured, and non-comprehensive. The aim of this chapter was not to establish a new methodology from scratch but rather to build on an existing state-of-the-art risk management standard. Introducing ISO 31000:2018 to the management of risks from biosecurity sensitive research would ensure a consistent, structured, and comprehensive risk approach to the management of biosecurity risks in research.

References

Arnason G (2017) Synthetic biology between self-regulation and public discourse: ethical issues and the many roles of the ethicist. Camb Q Health Ethics 26(2):246–256. https://doi.org/10.1017/S0963180116000840

Aubin Y, Idiart (2011) A export control law and regulations handbook: a practical guide to military and dual-use goods trade restrictions and compliance. Kluwer Law International, Netherlands

Becker G (2012) The "H5N1 publication case" and its conclusions. Acta Biochim Pol 59 (3):441–443

Bielecka A, Mohammadi AA (2014) State-of-the-art in biosafety and biosecurity in European countries. Arch Immunol Ther Exp 62(3):169–178. https://doi.org/10.1007/s00005-014-0290-1

Corera G (2009) Shopping for bombs: nuclear proliferation, global insecurity, and the rise and fall of the A.Q. Khan network. Oxford University Press, Oxford

Enserink M (2012) Will Dutch allow 'Export' of controversial flu study? Science 336(6079):285. https://doi.org/10.1126/science.336.6079.285

Hunter P (2012) H5N1 infects the biosecurity debate: governments and life scientists are waking up to the problem of dual-use research. EMBO Rep 13(7):604–607

International Organisation for Standardization (2018) ISO 31000:2018 risk management – guidelines. Geneva. https://www.iso.org/standard/65694.html

International Standardization Organisation (2018) ISO 35001: biorisk management for laboratories and other related organizations. https://www.internationalbiosafety.org/index.php/news-events/news-menu/news-items/571-iso-35001-biorisk-management-for-laboratories-and-other-related-organizations

Koblentz GD, Klotz LC (2018) New pathogen research rules: gain of function, loss of clarity. Bull At Sci. https://thebulletin.org/2018/02/new-pathogen-research-rules-gain-of-function-loss-of-clarity/

McQueen G (2014) Terror and the patriot act of 2001, implemented in the immediate wake of 9/11. Global Research. https://www.globalresearch.ca/terror-and-the-patriot-act-of-2001-implemented-in-the-immediate-wake-of-911/5400910

National Research Council (2010) Responsible research with biological select agents and toxins. National Academies Press, Washington, DC

Patrone D, Resnik D, Chin L (2012) Biosecurity and the review and publication of dual-use research of concern. Biosecur Bioterror 10(3):290–298. https://doi.org/10.1089/bsp.2012.0011

Rath J (2014) Rules of engagement. EMBO Rep 15(11):1119–1122

Rath J, Ischi M, Perkins D (2014) Evolution of different dual-use concepts in international and national law and its implications on research ethics and governance. Sci Eng Ethics 20 (3):769–790

Selgelid MJ (2016) Gain-of-function research: ethical analysis. Sci Eng Ethics 22(4):923–964

World Health Organisation (2006) Biorisk management: laboratory biosecurity guidance. World Health Organization 2006, WHO/CDS/EPR/2006.6

World Health Organisation (2010) Responsible life sciences research for global health security: a guidance. World Health Organisation WHO/HSE/GAR/BDP/2010.2. http://apps.who.int/iris/bitstream/handle/10665/70507/WHO_HSE_GAR_BDP_2010.2_eng.pdf?sequence=1