SANDIA REPORT
SAND2009-8070
Unlimited Release
Printed December 2009

Strengthening Risk Governance in Bioscience Laboratories

Jennifer Gaudioso[*], Susan A. Caskey[*], LouAnn Burnett[+], Erik Heegaard[#], Jeffery Owens[**], and Philippe Stroot[++]

[*] International Biological Threat Reduction Program, Sandia National Laboratories, Albuquerque, NM, USA
[+] Independent consultant, Franklin, TN, USA
[#] Biosecurity Institute, Lyngby, Denmark
[**] DLS Inc, Atlanta, GA, USA
[++] Xibios Biosafety Consulting, Brussels, Belgium

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia is a multiprogram laboratory operated by Sandia Corporation,
a Lockheed Martin Company, for the United States Department of Energy's
National Nuclear Security Administration under Contract DE-AC04-94AL85000.

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831
Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.osti.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd.
Springfield, VA 22161
Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.fedworld.gov
Online order: http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online

SAND2009-8070
Unlimited Release
Printed December 2009

Strengthening Risk Governance in Bioscience Laboratories

Jennifer Gaudioso[*], Susan A. Caskey[*], LouAnn Burnett[+], Erik Heegaard[#], Jeffery Owens[**], and Philippe Stroot[++]

[*] International Biological Threat Reduction Program, Sandia National Laboratories, Albuquerque, NM, USA
[+] Independent consultant, Franklin, TN, USA
[#] Biosecurity Institute, Lyngby, Denmark
[**] DLS Inc, Atlanta, GA, USA
[++] Xibios Biosafety Consulting, Brussels, Belgium

Abstract

Laboratories that handle dangerous pathogens need to manage their safety and security risks in a responsible manner. This need was highlighted in the December 2008 *World at* Risk report, which specifically called for bioscience laboratories that handle dangerous pathogens to implement a unified laboratory biorisk management framework to enhance their safety and security. This report is intended to help facility managers and policy makers better understand risk governance approaches for laboratories that handle dangerous pathogens. It identifies key drivers for implementation of biorisk management programs, and articulated possibilities for monitoring effective implementation of biorisk management programs. The report also addresses issues necessary to adequately and sustainably manage these biorisks.

TABLE OF CONTENTS

ACRONYMS

AAAS – American Association for the Advancement of Science
ABSA – American Biological Safety Association
BSL – Biosafety Level
BPRP – Biological Personnel Reliability Program
CEN – European Committee for Standardization
CDC – Centers for Disease Control and Prevention
CFR – Codes of Federal Regulation
CWA – CEN Workshop Agreement
DOE – Department of Energy
DOD – Department of Defense
EHS – Environmental Health and Safety
ERM - Enterprise Risk Management
IRGC – International Risk Governance Council
ISO – International Organization for Standardization
MC&A – Material Control & Accountability
MCDA – Multi-Criteria Decision Analysis
NAS – National Academies of Science
NRP – Notification and Response Protocol
NSABB – National Science Advisory Board for Biosecurity
PRP – Personnel Reliability Program
WHO – World Health Organization

DEFINITIONS[1]

Accident – an unintentional incident that results in harm

Biological agent – any microorganism including those which have been genetically modified, cell cultures and endoparasites, which may be able to provoke any infection, allergy or toxicity in humans, animals or plants

Incident – any undesired event that adversely affects completion of a task (in conducting research with biological agents and toxins) or causes harm

Laboratory biosafety – set of containment measures, technologies and practices that are implemented to prevent the unintentional exposure to biological agents and toxins, or their accidental release

Laboratory biosecurity – set of measures aiming at the protection, control and accountability for biological agents and toxins within laboratories, in order to prevent their loss, theft, misuse, diversion of, unauthorized access or intentional unauthorized release

Near miss – an incident that does not result in exposure, release, theft, sabotage, or loss of biological agents or toxins

Serious incident – an incident that results in exposure, accidental release, loss, theft, misuse, diversion of, or intentional unauthorized release of biological agents or toxins

[1] These definitions have been adapted from CWA 15793:2008 Laboratory Biorisk Management Standard, the International Risk Governance Council, and the U.S. National Safety Council to encompass, where appropriate, both safety and security concerns for biological risks.

ACKNOWLEDGMENTS

We would like to acknowledge the contributions of our colleagues across Sandia National Laboratories, including: Paula Austin, Mary Lynn Garcia, Debbie Haycraft, Nikki Held, Karl Horak, Jessica Jones, Daniel Lowe, Catherine Pasterczyk, Carlos Salazar, Reynolds Salerno, Teresa Torres, and Eric Wallace. They engaged us in debates, pointed us in the right direction, helped research topics, set up a project web portal to facilitate our collaboration, reviewed the BioRAM model, and/or drafted sections of this report. We would also like to acknowledge Sandia National Laboratories' Laboratory Directed Research and Development funding for support of this project.

EXECUTIVE SUMMARY

Laboratories that handle dangerous pathogens need to manage their safety and security risks in a responsible manner. This need was highlighted in the December 2008 *World at Risk* report, which specifically called for bioscience laboratories that handle dangerous pathogens to implement a unified laboratory biorisk management framework to enhance their safety and security. Currently, many laboratories rely on ad hoc programs or management systems to address these biorisks; this report analyzes the value in implementing integrated formal biorisk management systems in accordance with the *World at Risk* recommendation. Although safety and security pose separate risks and must be assessed independently, the system to manage these risks must be cohesive and unified to be effective from the laboratory perspective. A risk management framework has seven main phases: pre-assessment, risk assessment, concern assessment, risk characterization, risk evaluation, decision making, and implementation. The bioscience community has tools for implementation and is developing tools for risk assessment. This report will explore aspects of the other elements, especially approaches for pre-assessment and risk management. The ultimate goal of a biorisk management system should be to ensure an organization's biorisk management objectives are met in the most efficient and effective way; this report hopes to help institutions working towards this goal.

The report also identifies key technical approaches and gaps in the current state of the art that are crucial for laboratories adopting a formal biorisk management system. Risk assessment methodologies and metrics for measuring the effectiveness of any biorisk management system that is implemented are two significant areas where biosafety and biosecurity professionals currently lack structured tools. Other critical elements of good biorisk management programs include personnel reliability programs and training. This report makes specific technical recommendations on how to approach those issues in part by analyzing how risks are managed in other industries.

Biorisk management is also recognized as a major aspect of the development and sustainability of biological activities. The situation may be more crucial in some developing countries that are launching new activities involving biological risk without having the regulatory environment and without experience of biorisk management. The present report describes the situation and identifies processes, knowledge and skills that are needed to ensure the sustainability of biorisk management, looking successively at (1) the decision of launching activities implying some level of biorisk, (2) the design and construction of the biocontainment facilities needed to carry out the activities, and (3) the management of laboratory biorisks during the operational activities.

Biorisk management ideally provides a pact between authorities, the public, and the scientific community establishing trust and societal safety and security, while enabling the continued progress of science. The level of regulation by authorities

should be proportional to the risks. To achieve this, there needs to be a good understanding across sectors and communities to give a meaningful level of control and fit with daily operations.

INTRODUCTION

Managing biological safety and security risks is a sometimes difficult and costly endeavour. A comprehensive system incorporating the most important aspects of biosafety and biosecurity (i.e. biorisk), which encompasses both policy and management aspects, is necessary. On the institutional level a policy must be formulated, which addresses and shapes the overriding commitment (top down). The policy should be endorsed by the executive management. On the operational level, a customized management system should subsequently be developed, implemented and continually audited. A range of educational and awareness raising activities are needed to ensure a better understanding, compliance and ownership from everybody involved (bottom up). These activities come at a cost, albeit there may be a return on investment, depending on the type of operations and current standards. This report aims to present the bioscience community with approaches and tools commonly used for managing other risks to determine if any of those are applicable and helpful to managing laboratory biorisks. The topics explored in this study are primarily relevant to laboratories seeking to employ best practices but, because the public is increasingly concerned with whether bioscience laboratories handle pathogens and toxins responsibly, policy makers may also find this report helpful as they examine many of these same issues.[2] The annotated bibliography in Appendix G summarizes some of these key policy initiatives and reports.

Risk governance[3] aims at providing a framework for an organization to enable risk assessment and risk management activities to take place in a sustainable way. While improving decision making, planning and prioritisation, it contributes to a more efficient allocation and use of the resources within an organization. From this standpoint, risk management is seen as a process that creates value by ensuring that the resources consumed by risk management and control are used efficiently to guarantee the sustainability of the activities and the achievement of the strategic objectives. Risk governance should appear thus as a central part of any organization's strategic management.

Risk governance is based on thorough risk assessment, sound decision making, strict and consistent implementation of appropriate risk mitigation measures, monitoring and reviewing.

---

[2] Trans-Federal Task Force on Optimizing Biosafety and Biocontainment Oversight; *World At Risk* Report, WMD Commission, December 2008, http://www.preventwmd.gov; WMD Prevention and Preparedness Act of 2009, US Senate; EU CBRN Action Plan, http://ec.europa.eu/justice_home/news/.../com_2009_0273_annexe_2_en.pdf

[3] White paper on Risk Governance, The International Risk Governance Council, 2006 http://www.irgc.org/The-IRGC-risk-governance-framework,82.html.

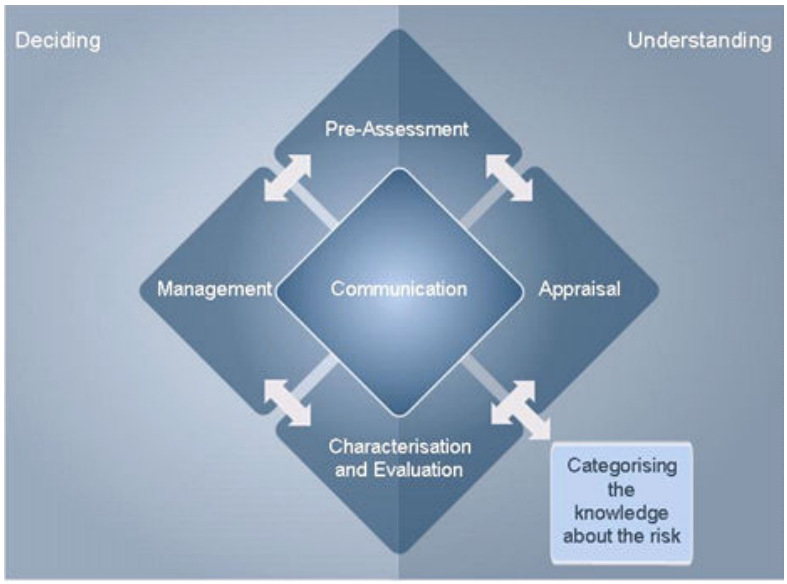


Figure 1. Risk governance process[4]

Biorisk management is also based on risk assessment[5]. Biological risk assessment is a legal obligation in many countries that have biosafety regulations[6], as part of the notification or authorisation process and/or as a basis to determine the required containment levels and other protective or preventive measures. It is also a major element of the WHO laboratory biosafety manual and a basis of the laboratory biorisk management standard CWA 15793[7].

The laboratory biorisk management standard CWA 15793, which is based on a management system approach like ISO 9001, ISO 14001 or OHSAS 18001, is intended to help laboratories develop a systematic framework for managing their risks. First, it requires a policy statement, which puts forth a strategic positioning and a formal commitment from the organization's top management. Secondly, biosecurity is included in the whole risk management approach together with biosafety. Last but not least, the planning phase is not limited to the risk assessment, but also includes planning for the resources needed for the implementation of the decisions and the monitoring of their outcome, which appears as some guarantee for a sustainable management. In general, key features of all management systems[8] include structuring the system to achieve the

[4]White paper on Risk Governance, The International Risk Governance Council, 2006 http://www.irgc.org/The-IRGC-risk-governance-framework,82.html.
[5]Terms used in relation to risk assessment are based on those of draft ISO Guide 73, "Risk management - Vocabulary", 2009 (http://www.npc-se.co.th/pdf/iso31000/ISO_DGuide_73_(B).pdf).
[6] National regulations implementing Directives 90/219/EEC (now replaced by 2009/41/EC) and 2000/54/EC in the European Union; "Regulation on the Biosafety Management of Pathogenic Microbiology Laboratories", 2004, in China; “Biological Agents and Toxins Act,” Singapore 2005.
[7]"Laboratory biorisk management standard", CWA 15793:2008 (ftp://ftp.cenorm.be/PUBLIC/CWAs/wokrshop31/CWA15793.pdf).
[8] www.iso.org

organization's objectives in the most effective and efficient way, understanding the interdependencies between the processes of the system, structuring approaches to harmonize and integrate processes, providing a better understanding of the roles and responsibilities necessary for achieving common objectives (and reducing cross-functional barriers), understanding organizational capabilities and establishing resource constraints prior to action, targeting and defining how specific activities within a system should operate, and continually improving the system through measurement and evaluation. All of these management system elements are applicable to managing laboratory biorisks and their implementation can be enhanced through a risk governance framework.

Risk governance provides an approach that is applicable to initial decision making. As stated in the IRGC Risk Governance Framework[9], risk assessment is preceded by a pre-assessment step aiming at providing a structured definition of the problem and identifying how it may best be handled. It supposes capturing a variety of issues at a strategic level, without omitting any of the risk-related factors that could have a significant impact on the activities. Pre-assessment includes a "risk framing" that ensures a common understanding of the risk issues by all stakeholders. The next step, risk appraisal, includes a technical risk assessment as well as a concern assessment that aims at identifying the perception of the stakeholders as well as possible sociological, economical and political consequences and implications. Results of the risk appraisal are then judged regarding risk tolerability and acceptability, which corresponds to risk evaluation according to the ISO terminology[10]. Decisions are made on this basis, and implementation of the risk management approach is then carried out accordingly. Communication is a major component of the whole process.

As part of the larger goal of strengthening laboratory biorisk management, the IRGC Risk-Governance framework offers an important structure for understanding that societies have different organizational capabilities for assessing and mitigating biorisks as well as different societal notions of what biorisk embodies. As such, the IRGC framework is useful for discussing the challenges to implementing a international norm of biorisk governance from both organizational and a political perspectives.

Organizational Capacity

The IRGC report acknowledges that, in the international context, the organizational capacity to fully assess risk as laid out by the framework is likely less than optimal. This is an especially pertinent observation for the implementation of a global biorisk management culture as some of the countries that nowadays have the fastest growing biotechnology and biology sectors and, as such, the greatest need for

[9] http://www.irgc.org/IMG/pdf/IRGC_WP_No_1_Risk_Governance__reprinted_version_.pdf
[10] http://www.npc-se.co.th/pdf/iso31000/ISO_DGuide_73_(B).pdf.

support in implementing proper biorisk management, are countries that have underdeveloped organizational capacity.

Furthermore, the process of risk framing, assessment, and evaluation may be subjected to various amounts of political forces that may wish to alter a risk assessment in order to further their own agendas. While the IRGC framework does not address the potential of political bodies using risk assessment to their advantage, the framework instead seeks to strengthen the entities conducting the assessments so that they can better withstand these pressures. In order to increase the organizational capacity of these agencies, the IRGC framework identifies three important variables for assessing the organizational capacity: assets, skills, and capabilities. The framework defines assets as the capabilities that form "the social capital for risk governance in the form of knowledge bases and structural conditions for effective management." Assets are then further broken down into four categories (1) rules, norms, regulations; (2) resources; (3) competencies and knowledge; (4) organizational integration. These assets are critical for any organization in their assessment of risk but also in their ability to control risks. The key element of these capabilities is organizational integration. The framework claims that without an organizational integration capacity the other factors would be "nullified." These assets are running threads throughout this report: for example, regulations and norms are important drivers for implementing biorisk management systems; organizational integration is a key outcome of implementing a good biorisk management system; and one of the main objectives of this report is to help facilities identify approaches to sustainable biorisk management, which necessarily requires appropriate resources, competencies, and knowledge.

The second variable identified is skills, which are defined as: "the quality of institutional and human performance in exploring, anticipating and dealing with existing and emerging risks." The skills should build upon and enhance the available assets of an organization. Essentially "skills" allow organizations to adapt to changing circumstances with greater continuity. The framework sees three skills as instrumental to this process: flexibility, vision, and direction. The need to be able to adapt to changing circumstances in the biorisk community is perhaps exemplified by the shift from a focus on laboratory biosafety to laboratory biorisks, now incorporating laboratory biosecurity concerns.

The third variable is capabilities, which are defined as: "the institutional framework necessary to translate assets and skills into successful policies. These three components constitute the backbone of institutional capacity for risk governance." The framework lays out several factors that form an additive structure of capabilities. These include relations, networks, and regimes. In general, these capabilities allow for the communication and implementation of risk-governance policies. Most institutions already recognize the importance of building skills for managing biorisks but perhaps struggle with developing effective mechanisms for skill development (see section on Training). Because communication is critical, often carried out ineffectively, and technology is rapidly expanding our tool set for

communicating, this report includes a dedicated section on exploring new tools for enhancing communication and how those tools might apply to different communication needs in support of a biorisk governance framework.

The IRGC method of identifying and categorizing important organizational capacities is extremely useful for analyzing different organizational structures as it not only identifies important institutional factors but also recognizes the importance of human factors in the development of independent and proficient biorisk governance organizations.

Political Culture

While IRGC framework for organizational capacity tries to develop an environment where organizations responsible for risk governance can work with some independence from the endogenous political culture, it is impossible to entirely remove the effects of political culture from risk management. Thus, the IRGC framework also provides a means of identifying the type(s) of political cultures that exist within a particular setting so that a better understanding of the entire biorisk environment can be developed.

Due to large differences of governmental style from country to country, countries necessarily have different pathways for dealing with risk, which makes prescriptive and "one size fits all" approaches to managing biorisks unrealistic. The IRGC framework categorizes governmental styles to facilitate a greater understanding of these styles and the ways in which risk is approached within each type of style (the "approaches are "pure types" and should not be expected to be found, as laid out, in any one setting). Although the globalization of certain aspects of risk management has reduced the amount of variability brought by nationality and cultural background, there are still several components that vary due to these differences. The IRGC frameworks lists three such components that vary based upon "national culture, political traditions, and social norms" they are: systemic knowledge, legally proscribed procedures and social values. A good example of the global discrepancy in risk management was documented in a recent comparison[11] of US and European Union regulatory approaches to 100 different risks from 1970 – 2004. Swedlow et al showed that, on average, the US had greater relative regulatory precaution than Europe from 1970 through the late 1980s while Europe adopted a relatively more precautionary approach to regulating risks during the 1990s through the early 2000s. Culture and social norms also influence what may be appropriate for vetting individuals (see section on Personnel Reliability Programs).

[11] Swedlow, B., D. Kall, Z. Zhou, J.K. Hammitt, and J.B. Wiener, "Theorizing and Generalizing about Risk Assessment and Regulation through Comparative Nested Analysis of Represented Cases," Law & Policy, 31(2), 236-269, 2009.

Attempting to clarify the way in which these components can affect a country's approach to risk management, the IRGC classifies four different governmental styles:

- *Adversarial* approach "is characterized by an open forum in which different actors compete for social and political influence in the respective policy arena."
- *Fiduciary* approach is "the decision making process is confined to a group of patrons who are obliged to make the 'common good' the guiding principle of their action."
- *Consensual* approach "is based on a closed circle of influential actors who negotiate behind closed doors. Social groups and scientists work together to reach a predefined goal."
- *Corporatist* approach "is similar to the consensual approach, but is far more formalized. Well-known experts are invited to join a group of carefully selected policy makers representing the major forces in society (such as the employers, the unions, the churches, the professional associations, the environmentalists)."

These differing governmental styles lead to different types of risk management processes and points of emphasis. For example, the main risk management emphasis of the adversarial approach is "mutual agreement on scientific knowledge and pragmatic knowledge" while within the corporatist approach the main emphasis is "on expert judgement and demonstrating political prudence." While not strikingly different or opposing, these two different types – and all the approaches listed above – demonstrate different practices that are worth noting. Furthermore, by understanding which of the above categories are applicable, a biorisk governance program is likely to find greater acceptance and penetration within a governmental or non-governmental institution and could likely lead to more successful and sustainable implementation.

THE CASE FOR STRENGTHENING RISK GOVERNANCE

According to risk governance precepts,[12] risk management starts with a pre-assessment that should include the following steps:

- problem framing, in order to reach a consensus on the risks to be addressed among all stakeholders;
- early warning and monitoring, essentially asking whether there are signals institutions can and should monitor;
- pre-screening, in order to categorize the risks, select the best risk assessment method, and then manage them;
- and selection of conventions and rules for assessing the risks and concerns.

[12] "White paper on Risk Governance", The International Risk Governance Council, 2006 (http://www.irgc.org/The-IRGC-risk-governance-framework,82.html).

At least some of these pre-assessment concepts may be particularly relevant and currently neglected in efforts to manage laboratory biorisks. The public, policymakers, and scientists often have very different understandings on the risks associated with working with biological agents and there are instances where neglecting to take the views or concerns of some of these parties into consideration has led to delays or failures in the launch of some activities.[13] In a later section of this paper, we will explore incident reporting approaches and other possible indicators for monitoring biorisks. Pre-screening will be discussed in the risk assessment section of this report; at the highest level, laboratory biorisks are typically categorized as either biosafety risks (accidental) or biosecurity risks (intentional). A gap in many biorisk assessments is the failure to fully document those assessments. For example, assessments often neglect to explicitly state many of the conventions underlying their assessments, such as applying animal data on infectious dose to assessing risks for human laboratory workers.

This section will explore some of the mechanisms that the biorisk community uses to identify biorisks, frame the problem, and understand what factors might drive a facility to implement a formal biorisk management system.

Review of Biorisk Cases

A better understanding of what types of undesired events have actually occurred in the recent past is an important pre-requisite for framing the biorisk problem and for a more informed discussion on how to better manage those identified risks. Appendix A contains brief summaries of a variety of biorisk cases, illustrating real-life problems with biosafety and biosecurity. However, such information on biorisk cases is scarce and rarely accessible outside the directly concerned spheres. This lack of publicly available data prohibits a statistical analysis and inference on possible causes. Nevertheless, commonalities across many of the cases can be identified. To facilitate comparison, the cases in Appendix A are grouped according to laboratory exposures (actual or potential), unintentional releases from the facility, theft, inappropriate shipments, inventory discrepancies, unauthorized access, unauthorized experiments, inadequate biosafety measures, inadequate biosecurity measures, problems with documentation, and inadequate training.

As discussed in more detail later in this report, KATTAR[14] (Knowledge, Assignment, Training, Tools, Accountability, and Resources) is one example of a framework that can help evaluate incidents and then develop recommendations for improving biorisk management programs. Many of the KATTAR elements can be seen in the cases reviewed as part of this study. For example, in the 2003 incident

[13] "BU biosafety lab ignites critiques" The Tufts Daily, October 20, 2009. http://www.tuftsdaily.com/bu-biosafety-lab-ignites-critiques-1.2028407

[14] Lundberg, J., Rollenhagen, C., & Hollnagel, E. What-You-Look-For-Is-What-You-Find - The consequences of underlying accident models in eight accident investigation manuals. *Safety Science, in press*, 2009.

of laboratory-acquired infection of SARS in Singapore, the incident investigation identified insufficient training as a root cause.[15] Texas A&M had issues with accountability in their select agent research program (including multiple cases of unauthorized access and conducting experiments without the requisite approvals).[16] The theme of poor biorisk program management underlies almost all of the reviewed cases.

While no system will ever be perfect, many of these examples could have been avoided with more attention to a systematic, unified biorisk management system as recommended by the WMD Commission report and, hence, explored in this report. The biorisk management system approach addresses all of the KATTAR elements: knowledge to effectively identify and manage the biorisks, appropriate assignment of roles and responsibilities, training people on the necessary biorisk mitigation procedures, ensuring that the appropriate tools are available, ensuring management is accountable for the biorisk management program, and having the appropriate resources on hand.

Drivers for Implementing Biorisk Management Systems

Determining biorisk drivers

In an effort to better understand the motivation behind implementing a biorisk management system, we looked at some of the governing mechanisms involved. For many safety issues, there is often a close relationship between the actor and the deemed risk, offering a vested personal interest. This allows for perhaps improved attention and better compliance on the operational level. In contrast, the security element is primarily driven by societal concerns, and thus often instigated through legislation or by a competent authority. Thus, security is often detached from the person involved and the risk which is being governed. However, based on a quick survey of international colleagues (Appendix E), both measures, including the specialized tasks of biosafety and biosecurity, are seemingly driven by internal aspirational factors (i.e. “pull”), and less on external imposed factors (i.e. “push”).

Through research of drivers in other risk management disciplines combined with an operational knowledge of biosafety and biosecurity, we identified a range of possible drivers for implementation of biosafety and biosecurity, and ultimately for implementing a biorisk management system, such as to comply with existing rules and regulations, meet accepted best practices, reduce the risk of economic loss, to satisfy public demands for transparency and ethical behavior, and to protect the community, workers, and the environment. Although there are commonalities between biosafety and biosecurity drivers, some of these drivers may be more important for one or the other or to different actors. For instance, the reasons why an institution's executive management may be interested in managing biorisks will likely be different from some of the reasons that laboratory workers may be

[15] Singapore Ministry of Health Review Panel, Biosafety and SARS Incident in Singapore September 2003.
[16] Letter from DSAT Director to Responsible Official, Texas A&M University, August 31, 2007.

concerned about how biorisks are addressed. In general, drivers for risk management can be broadly grouped into four categories:[17] strategic, financial, operational, and hazard. Each category can be sub-divided into internal and external drivers.

Categorizing Biorisk Drivers

Type	Internal (Pull)	External (Push)	Actor
Strategic Risks			
Industry/technical advances (inadvertent technology transfer)		X	Management
Innovation / novel research (potential high hazard)	X		Management Lab personnel
Ethics	X	X	Management Lab personnel Non-lab personnel
Market policy (uniform standards / level playing field)	X		Management
Public image		X	Management
Financial Risks			
Reduce risk of fines and other sanctions		X	Management
Economic loss (lost business)		X	Management
Attract or maintain research funding	X		Management Lab personnel
Operational Risks			
Comply with rules and regulations (national and international requirements)		X	Management

[17] "A Risk Management Standard" compiled by The Institute of Risk Management, the Association of Insurance and Risk Managers, and ALARM The National Forum for Risk Management in the Pubic Sector. 2002. http://www.theirm.org/publications/PUstandard.html

Type	Internal (Pull)	External (Push)	Actor
Comply with biorisk guidance (WHO, BMBL, etc)		X	Management Lab personnel
Creating a safety and security culture	X		Management Lab personnel Non-lab personnel
Staff morale	X		Management Lab personnel Non-lab personnel
Business continuity	X		Management
Hazard Risks			
Community / public health		X	Management
Environment		X	Management
Theft (tangible items and intellectual property)	X	X	Management Lab personnel
Personnel health and safety	X		Management Lab personnel Non-lab personnel
Insider acting with ill intent	X	X	Management Lab personnel Non-lab personnel

As shown from the analysis in the above table on biorisk drivers, the primary target for engaging and communicating biorisk issues is the executive management group. From the management perspective, biosecurity is probably primarily viewed as an enterprise risk management issue, with special attention to the financial and business continuity risks. A secondary objective is complying with existing regulations. In the most effective biorisk management systems, once there is institutional buy-in on the need to address biosecurity, other members of the organization may be involved. This is likely to be more sustainable than if biosecurity is simply addressed through an ad hoc bottom up approach by concerned individuals within an institution.

Yet, biosecurity and biosafety are currently probably best known in traditional professional biosafety and Environmental Health and Safety (EHS) circles and not seemingly well recognized on the management group level. However, it is

management that needs to sign onto the concept, before substantial progress can be made. As noted by the IRGC, sound risk governance can minimize many aspects of risks, such as the cost of inefficient regulations or a tarnished institutional image.

The types of drivers identified in this section were presented to a small group of international biosafety professionals (Appendix E), who were asked to rank their main reasons or drivers for implementing biorisk policies and management systems from both a biosafety and a biosecurity perspective. The top drivers identified by the survey respondents are captured in the table below. Significantly, the top motivating factor for both laboratory biosafety and biosecurity was to protect the community, environment and workers, although more respondents identified this as their primary driver for biosafety than biosecurity. Also common to both biosafety and biosecurity was the identification of the desire to develop a culture of responsibility (safety and security culture) as an incentive to implementing biosafety and biosecurity. Most respondents listed compliance with rules and regulations as one of their top three drivers.

Top Three Biosafety and Biosecurity Risk Drivers (n=17)

RANK	BIOSAFETY	BIOSECURITY
1	**53% - To protect the community, environment, and workers** 35% - To comply with rules and regulations 6% - To comply with guidance documents 6% - To ensure business continuity	**35% - To protect the community, environment, and workers** 29% - To reduce the risk of theft of materials 29% - To comply with rules and regulations 6% - To comply with guidance documents
2	**35% - To build a safety and/or security culture** 23% - To comply with rules and regulations 12% - To protect the community, environment, and workers 12% - To comply with guidance documents 6% - To reduce the risk of theft of materials 6% - To attract, maintain, or increase research funding 6% - To satisfy public demand for transparency or ethical behavior	**23% - To build a safety and/or security culture** 18% - To comply with rules and regulations 12% - To comply with guidance documents 12% - To reduce the risk of theft of materials 12% - To attract, maintain, or increase research funding 12% - To reduce the risk of a tarnished institutional image 6% - To ensure business continuity 6% - To protect the community, environment, and workers
3	**23% - To comply with rules and regulations** 18% - To comply with guidance documents 18% - To meet internally accepted best practices 12% - To reduce the risk of a tarnished institutional image 6% - To satisfy public demand for transparency or ethical behavior 6% - To build a safety and/or security culture 6% - To ensure business continuity 6% - To reduce the risk of theft of materials	**23% - To reduce the risk of theft of materials** 18% - To comply with guidance documents 18% - To meet internally accepted best practices 12% - To protect the community, environment, and workers 6% - To comply with rules and regulations 6% - To reduce risk of economic loss 6% - To satisfy public demand for transparency or ethical behavior 6% - To build a safety and/or security culture 6% - To ensure business continuity

Regulatory drivers

Although our cursory survey identified regulatory drivers as a notable mechanism for incentivizing biorisk management, few countries have a regulatory framework that addresses laboratory biorisks at the operational level. Bioscience laboratories may be impacted by national legislation to implement the Biological and Toxin Weapons Convention,[18] United Nations Security Council Resolution 1540, and international agreements on export controls (e.g. Australia Group). If addressed through regulations, biosafety and biosecurity appear to be addressed as separate concepts and not in an integrated biorisk approach. It can be hard to track down relevant information on legislative initiatives but several organizations have compiled information on national level legislation: The Verification Research, Training and Information Centre (VERTIC) built an online database of BWC implementing legislation based on their research;[19] the Organization for Economic Cooperation and Development (OECD) maintains a website with a listing of biological legislation on security, biosafety, bioterrorism, biological weapons, import and export controls, and biodiversity;[20] and Interpol summarizes legislative measures that address counterterrorism and the regulation of biology.[21]

In countries that have biosafety regulations, especially in the developing world, , biosafety is often regulated primarily because of concerns over genetically-modified organisms and the management of the risks related to non-modified pathogens is not taken into consideration. In other countries, biosafety is implemented primarily through guidance rather than binding regulations. Since biosecurity is much newer, it is not surprising to find that few countries currently have national legislation requiring laboratories to implement laboratory biosecurity measures. Europe is a good indicative example in many ways since the European Union (EU) comprises 27 independent countries but the European Commission (EC) has funded a coordination action[22] "to promote European harmonization and the exchange of practices relating to biosafety and biosecurity management of biological containment facilities." The EC has issued three main biosafety directives (2000/54/EC, 2001/18/EC, and 2009/41/EC) but has no directive specific to biosecurity. As a result, all of the EU countries have biosafety legislation implementing the EC biosafety directives but only the UK, France, the Czech Republic and more recently Denmark[23] have specific legislation on biosecurity

In contrast, the US does not have explicit biosafety legislation. However, US bioscience institutions must meet the Department of Labor's Occupational Safety and Health Administration (OSHA) General Duty Clause "to provide their employees with a workplace free from recognized hazards likely to cause death or

[18]BWC Implementation Support Unit, National Implementation Database,
[19] http://www.vertic.org/datasets/bwlegislation.asp
[20] http://www.biosecuritycodes.org/leg.htm
[21] http://www.interpol.int/Public/BioTerrorism/NationalLaws/
[22] http://www.biosafety-europe.eu/
[23] Entered into force on November 1, 2009. Center for Biosecurity and Biopreparedness, Statens Serum Institute, http://www.biosikring.dk/

serious physical harm."[24]The US National Institutes of Health (NIH) requires institutions receiving funding for recombinant DNA to be in compliance with the NIH Guidelines for Research Involving Recombinant DNA Molecules.[25] Many institutions follow the guidelines as best practice even if they are not required to meet them since they are not required for institutions not receiving NIH or other funding that makes these guidelines a pre-requisite. Compliance with the US Biosafety in Microbiological and Biomedical Laboratories guidelines[26] is a legal necessity for institutions that work with select agents. Select agents are also the only agents legally subject to biosecurity controls under the US national biosecurity legislation (authorized by the Public Health Security and Bioterrorism Preparedness and Response Act of 2002). The implementing regulations[27] regulate biological agents and toxins ("select agents") that potentially pose a severe threat to public, animal, and plant health and safety.

A few other countries have also started to develop laboratory biosecurity regulatory systems (e.g. Australia, Canada, Japan, and Singapore) providing some opportunities for sharing lessons learned and international collaboration to determine the best path forward for effective and functional regulations. Successful adoption and implementation of laboratory biorisk legislation requires a fine-tuned interplay between all stakeholders, especially the authorities and regulated entities. Biorisk management ideally provides a pact between authorities, the public and the scientific community establishing trust and societal safety and security, while enabling the continued progress of science. The level of regulation by authority should be proportional to the risks. To achieve this, there needs to be a good understanding across sectors and communities to give a meaningful level of control and fit with daily operations.

ASSESSING BIOLOGICAL RISKS FOR LABORATORIES

The leading guidelines on laboratory biosafety and biosecurity, such as the WHO Laboratory Biosafety Manual and the US Biosafety in Microbiological and Biomedical Laboratories, all emphasize that risk assessment is the fundamental planning step for managing these risks. They outline risk assessment principles but do not provide detailed guidance or suggested methodologies for conducting risk assessments. In an informal survey of 24 respondents from 14 countries (see Appendix D), 10 indicated that they were not doing any risk assessments and, of those doing assessments, no one described a methodology. This limited data supports our understanding of the current "state of the art" of laboratory biorisk

[24] OSHA Act of 1970.
http://www.osha.gov/pls/oshaweb/owadisp.show_document?p_id=3359&p_table=OSHACT
[25] http://oba.od.nih.gov/oba/rac/guidelines_02/NIH_Guidelines_Apr_02.htm
[26] US Department of Health and Human Services, Centers for Disease Control and Prevention and National Institutes of Health, Fifth edition, February 2007.
http://www.cdc.gov/od/OHS/biosfty/bmbl5/bmbl5toc.htm
[27] CDC Select Agent Regulations (42 CFR Part 73) and APHIS Select Agent Regulations (7 CFR Part 331 and 9 CRF Part 121). http://www.selectagents.gov

assessments. In general, these assessments are ad hoc, relying on individual expertise and experiences.

Biological risk assessment appears generally as a two-step technical approach, based on (1) the hazard or risk identification involving the characterization of the biological agents or materials (often on the basis of official lists and procedures) and the evaluation of their potential impact, and (2) a risk analysis of the activities. The result of the risk assessment determines the biological containment level that is required, together with possible additional measures aiming at protecting the personnel, the external community and the environment. Biosecurity aspects are generally not included. Although most regulations leave room to possible adaptations and other alternative measures provided they are justified by risk assessment, decisions with respect to facility design or biosafety practices are often made on the basis of rather prescriptive standards and a box ticking approach, resulting in facilities and practices that may, in some circumstances, not be fully adapted to the needs of the organization and the actual level of risk. Technical elements that are not mentioned explicitly in the regulations, as for instance some important technical specifications, can be neglected while other more general issues such as biosecurity are sometimes omitted. Moreover, wider considerations like the influence of public perception, the impact of operating costs or the risk acceptance level are generally not really taken into account.

Because there is a general lack of good quantitative data for biorisk assessments, the risks are assessed by subject matter experts. However, a systematic approach in capturing and analyzing these inputs can make the assessments more robust; a Multi-Criteria Decision Analysis (MCDA) framework can be developed for these problems. MCDA is a quantifiable decision-making approach that is useful when there are numerous and conflicting criteria involved in a decision. MCDA aims to "link technological performance information with decision criteria and weightings elicited from decision-makers, allowing visualization and quantification of the trade-offs involved in the decision-making process."[28] This approach offers a systematic, explicit, and rigorous mechanism for eliciting and quantifying subjective judgments. One of the primary benefits of the MCDA approach is that it factors in the subjectivity of the decision makers, allowing for their personal preferences and experience to play a role in the final decision.

In complementary efforts, we have developed MCDA models for assessing biosafety and biosecurity risks; overviews of each are found in the following sections. Identifying the criteria is the most critical step in the development of those efforts since the criteria structures the problem for the rest of the elicitation and analysis. Human bias can be a large factor in using the criteria to evaluate the risks

[28] Linkov, F. K. Satterstrom, G. Kiker, T. Bridges, E. Ferguson, and J. Nelson, "Multi-Criteria Decision Analysis and Homeland Security Applications," Working Together: Research and Development (R&D) Partnerships in Homeland Security" Proceedings of 2005 Conference. Boston, 2005.

of a given situation. To mitigate this bias in the software tool, the risk assessor will answer a set of straightforward, multiple choice, and true/false questions; a numerical engine will translate the answers into the "scores." The look-up tables for generating these scores from the answers should be peer-reviewed prior to building the software tool.

To determine the relative weights of the criteria, the Sandia team conducted subject matter elicitations of biorisk experts. The Analytic Hierarchy Process (AHP) is used to assist the experts in assigning relative weights to the criteria. This mechanism has been selected since it is based on pair-wise comparisons of decision criteria, rather than utility and weighting functions. Expert Choice is an established software tool that performs these pair-wise comparisons, and it will be used to weigh these criteria. There are several key technical issues associated with eliciting quantitative judgments from subject matter experts: How do you quantify judgments? How do you combine inputs from multiple subject matter experts? In addition to expert judgment for the criteria weights, we will also rely on eliciting such input when data for scoring specific criteria is incomplete. Elicitation is inherently open to bias. For example, optimism is the tendency for experts to give answers that favor their desired outcomes. One approach to minimize bias is to decompose the complex problem (biorisk assessment) into simple elements.

The following two sections give short overviews of MCDA methodologies for assessing biosafety and biosecurity risks. Although there is considerable overlap between the two models, separate assessments of safety and security assessments are necessary, even if ultimately they are managed in an integrated framework. For example, there are many similarities in the undesirable events and possible consequences in safety and security assessments, however the initiating events (and, thus, the likelihoods) are different (accidental versus intentional).[29]

Biosafety Risk Assessment Methodology

Implementation of biosafety is generally based on a risk assessment, which historically has been a subjective and qualitative process that relies heavily on expert opinion and unique personal experiences. Many individuals who conduct biosafety risk assessments generally depend on pre-determined biological safety risk groups as the basis of their evaluations. Biological agents have been classified into biological safety risk groups[30] based upon their properties to cause infectious disease or other harm to the personnel, the community, livestock, or the environment. Such classification does not take into account the risk of accidental release or exposure in a particular laboratory during a particular experiment, which should be evaluated during the risk assessment of the laboratory activities. Different national and international organizations and experts have developed their

[29] M. K. Snell, "Probabilistic Security Assessments: How They Differ from Safety Assessments," SAND Report, 2002, SAND2002-0402C.
[30] For example: World Health Organization, Laboratory Biosafety Manual, 3rd edition, 2004.

own scheme for defining agent risk groups, leaving more or less freedom to the risk assessor to define the risk group according to possible specific characteristics (e.g. strain, modifications, and attenuation). Moreover, the risk also depends on how that agent will be used in the laboratory.

This risk assessment process is based entirely upon expert opinion of the hazards related to the biological agents and an ad-hoc evaluation of the risks related to the activities by the assessors. The results of such an assessment do not necessarily reflect new bioscience research, or biosafety technologies and methodologies in an adequate mannaer. Moreover, the results of such risk assessments are solely qualitative, highly variable, and not reliably repeatable. Many experts believe this is a significant problem, especially with the current rapid expansion in the number of high containment research facilities, and the increasing amount of work around the world with dangerous biological agents.

There is general consensus on the high-level risk assessment process, which can be broken down into three steps: identification of the biological agent or hazard and its unique biochemical properties; assessment of the probability of the hazard to cause an undesired event (exposure, disease etc.), the actual consequence; and management of the risk through established control measures and reassessment if necessary.

In partnership with the American Biological Safety Association and the Canadian Science Centre for Human and Animal Health, Sandia National Laboratories has been working to develop a biosafety risk assessment methodology to help the community migrate biosafety risk assessment from a qualitative, opinion-based method to a systematic, standardized methodology. The standardized biosafety risk assessment methodology that includes several elements: 1. Accepted criteria for assessing the risk, 2. A "scoring system" for evaluating the situation against the criteria, 3. Relative weights for the criteria since not all criteria will contribute equally to the risk, and 4. An equation that combines the criteria scores and the relative weights to produce a measure of the risk.

In the biosafety model, risk is defined as a function of the likelihood of infection by the agent, the likelihood of exposure through an infectious route and the consequences of disease assuming infection.

$$\mathbf{R} = F\,(\mathbf{L_i}, \mathbf{L_e}, \mathbf{C_d})$$

Likelihood of infection (L_i) is defined by the biological factors of the agent that influences the ability to cause infection. These include factors of transmissibility, agent stability, and also include infection mitigation measures, e.g. vaccine availability and effectiveness.

Likelihood of exposure (L_e) is defined by exposure hazards that exist in and around the specific activity with that agent. These factors are defined by a route of

exposure, e.g. percutaneous hazards. In place biosafety practices are included as exposure reduction measures.

Consequence of disease (C_d) is defined by the factors used to define disease in a specific host as based upon a normalized population. These factors include, for example, morbidity, mortality, and disease mitigation measures like effective and available anti-microbials.

Human biosafety risks to be assessed:

1. Risk to individuals performing direct manipulation to agent (in vitro and in vivo)
2. Risk to individuals working in same laboratory
3. Risk to persons within facility
4. Risk to community of primary exposure
5. Risk to community of secondary exposure

Animal biosafety risks to be assessed:

1a. Risk to animal community of breach of containment
2a. Risk to animal community of secondary exposure

Biosecurity Risk Assessment Methodology

Although it is a newer field and there is less precedent relative to biosafety, there is a general consensus among biosecurity experts that the implementation of laboratory biosecurity should also be based on a risk assessment (see, for example, CWA 15793 Laboratory Biorisk Management Standard, US Select Agent regulations,[31] and the WHO Laboratory Biosecurity Guidance). Unsurprisingly, there is even less information in the technical literature on biosecurity risk assessment approaches[32] than there is for biosafety risk assessment.

This section outlines an updated methodology for assessing biosecurity risks, i.e. the risk at a bioscience institution where the source of harm is deliberate; the source of harm may be theft, misuse, diversion, unauthorized access or intentional unauthorized release. The original methodology is outlined in the *Laboratory Biosecurity Handbook*.[33] Although laboratory biosafety and biosecurity risks are unique, there are many similarities in process, available data, and individuals involved, so not surprisingly, we rely on a similar methodology as the biosafety risk assessment methodology described above.

There are a range of biosecurity risks relevant to institutions, including:

[31] www.selectagent.gov
[32] R. M. Salerno and J. Gaudioso, CRC Laboratory Biosecurity Handbook, 2007.
[33] R. M. Salerno and J. Gaudioso, CRC Laboratory Biosecurity Handbook, 2007.

1. Risk that an agent is stolen from a facility and subsequently used to execute a bioterrorism attack[34]
    a. Risk to persons in area of attack (directly exposed in attack)
    b. Risk to human community from secondary exposure
    c. Risk to first responders
    d. Risk to perpetrator (accidental or deliberate self-infection)
    e. Risk to persons in vicinity of clandestine facility (e.g. lab, storage location) (biosafety accident during weaponization)
    f. Risk to persons at facility (non-pathogen risk) during adversary's attempted theft
    g. Risk to animals in area of attack (directly exposed in attack)
    h. Risk to animal community from secondary exposure
    i. Risk to plants in area of attack (directly exposed in attack)
    j. Risk to plant community from secondary exposure
    k. Risk to economy
    l. Risk to society
    m. Risk to facility (operational impacts if facility is suspected/identified as the source – shut down, liability)
    n. Risk to country if facility is suspected/identified as the source (e.g. international sanctions)
2. Risk that intellectual property is stolen (facility faces financial, operational, reduced market share impacts)
3. Risk that the facility is sabotaged
    a. By issue focused extremists just trying to shut down facility or free animals
    b. Sabotage designed to release pathogens

However, the model elucidated in this report will only address risks associated with theft and subsequent misuse of a biological agent to attack people or animals directly and through a secondary exposure (risks 1a, 1b, 1g, and 1h in the above list).

In the biosecurity model, risk is defined as a function of the likelihood that the facility will be targeted, the likelihood the agent can be used as a weapon, and the consequences of an attack with that agent.

$$\mathbf{R} = F\,(\mathbf{L_f}, \mathbf{L_a}, \mathbf{C_a})$$

Likelihood of theft from the facility (L_f) is defined by the facility biosecurity vulnerabilities (including physical security, personnel reliability, material control and accountability, information security, transportation security, and program management), the threat environment, and how unique the facility is as a pathogen source. The threat environment includes assessing the range of possible adversaries

[34] Biocrime (a small-scale attack, targeting only one to a few individuals) is really a subset of bioterrorism but may need to be recognized separately as a driver for institutions to implement biosecurity

(known and/or notional). The uniqueness of the facility as a source for a given pathogen considers both the availability of the pathogen in the environment and in other facilities plus the ease or difficulty in synthetic pathway (*de novo* synthesis or mutation of a related pathogen).

Likelihood agent can be used as a weapon (L_a) is defined by fundamental properties of the agent (transmissibility, stability), ease or difficulty to produce a suitable quantity of the agent in a suitable form, ease or difficulty in dispersing the agent, and the adversary's awareness of the agent). This set of criteria attempts to capture the effectiveness of the agent as a weapon.

Consequence of disease (C_a) is defined by the disease impacts, socioeconomic impacts, and impact of secondary transmission. Disease impacts are based on a specific host in a normalized population, including morbidity, mortality, and disease mitigation measures like effective and available anti-microbials.

Scalars are used to influence the magnitude of the risk value. In this biosecurity model, consequences are calculated based on the maximum credible consequences but the risk can be reduced through scalars for adversary motives (apocalyptic event, sicken voters ala Rajneeshees, etc) and for adversary capabilities (e.g. a less capable notional adversary could have the risk reduced by a scalar that accounts for their lesser ability to pull off a bioterrorism event).

Details on the Biosecurity Risk Assessment Methodology (BioRAM) can be found in Appendix C.

KEY ELEMENTS FOR MITIGATING BIORISKS

There are many important elements of a good biorisk management system[35], such as risk identification, risk assessment, biorisk management policies, roles and responsibilities, personnel, operational risk mitigation measures (e.g. primary barriers, personnel protective equipment, access controls, etc), inventories, waste management, incident response planning, and biorisk management reviews. But two important gaps, as evidenced by the biorisk cases in Appendix A, are the lack or insufficiency of appropriate training and personnel reliability programs. From our perspective, these gaps hold true across a wide range of bioscience institutions although these gaps may be more obvious in some academic settings with a large turn-over and in developing countries, given the overall lack of expertise in biorisk management. The importance of these issues has also been identified by many others, including the American Association for the Advancement of Science (AAAS) and the US National Academies of Science (NAS).

[35] CWA 15793, Laboratory biorisk management standard, 2008.

In March 2009, AAAS held a workshop on these issues and produced a report, Biological Safety Training Programs as a Component of Personnel Reliability[36] that highlighted the need for both initial and ongoing training. As noted earlier, there is a lack of formalized and systematic training in many institutions around the world. Initial training should definitely be provided in a systematic and documented manner. However, while using external resources are possible and appropriate for many aspects of initial training, refresher training is an on-going training that often has to be done in house. The timing of initial training is obvious yet the frequency of refresher training is less clear; the AAAS report did not recommend a specific frequency for the needed ongoing training. Since ongoing, refresher training takes time away from staff's time for their institution's core mission, it is important to strike a balance and train as needed without unnecessarily requiring training.

The NAS also recently released a report,[37] Responsible Research with Biological Select Agents and Toxins, examining the US Select Agent Program. This report recognizes the value of personnel reliability programs (PRP) and emphasizes the need to create a culture of trust and responsibility. There are also others in the US Executive Branch[38] and in Congress[39] looking at whether the Select Agent Program personnel reliability components should be strengthened. Although the NAS report endorses the current Select Agent Program mechanisms for screening personnel, personnel reliability programs are absent in much of the global bioscience enterprise.

Since an institution must address both of these key components as part of any effective biorisk management program, this section of the report reviews how other industries handle these issues. Some key principles have been identified that should translate from other industries and are discussed below for consideration at bioscience institutions.

---

[36] AAAS Center for Science, Technology and Security Policy and AAAS Program on Scientific Freedom, Responsibility and Law, Biological Safety Training Programs as a Component of Personnel Reliability, Workshop Report, 2009.

[37] NAS Committee on Laboratory Security and Personnel Reliability Assurance Systems for Laboratories Conducting Research on Biological Select Agents and Toxins; National Research Council, 2009. http://www.nap.edu/catalog/12774.html

[38] Presidential Executive Order 13486, Strengthening Laboratory Biosecurity in the United States, Federal Register, 74(9), Jan 14, 2009.

[39] WMD Prevention and Preparedness Act of 2009, 111th Congress, 1st session.

Effective Refresher Training[40]

Refresher training sessions held at determined intervals following initial training courses are essential in order to enhance skill retention and confidence in performance. However, requiring training with greater frequency than necessary for adequate performance can be detrimental to employee satisfaction, retention and recruitment, and can also result in unnecessary costs to employers. It is thus necessary to establish a timeline for refresher training that is based on a balance between the need for skill maintenance and the practicality of requiring numerous training courses.

The maintenance of skills will vary according to the specific task, as different types of skills are acquired and lost at different rates. Certain skills, such as those required to perform cardiopulmonary resuscitation (CPR), are more susceptible to decay and can begin to decline in a period as short as two weeks following initial training, with further decline continuing for about a year. Other skills such as riding a bike can be retained for years following original skill acquisition with very little practice. These differences can be explained by classifying tasks into skill sets. For example, physical and speed-based skills appear to be retained longer than cognitive and accuracy-based skills. Likewise, closed-loop skills, which involve discrete responses that have a definite beginning and end, are retained longer than open-looped skills, which involve continuous, repeated responses that have no definite beginning or end. The ideal refresher training schedule will reflect an understanding of the rate at which the particular skill to be trained is lost.

Studies have shown that the most consistent predictor of skill decay is the length of time between training and the use or practice of a skill. In the workplace, many skills acquired during training are only necessary intermittently and infrequently. It can logically be assumed that without regular, frequent use of a skill, forgetting will occur. Generally, if the task in question is regarded as important but is not performed frequently (such as CPR) refresher training should occur more frequently to counter skill decay. Tasks that are regarded as important but are performed more frequently (such as nurses giving shots) should be trained annually

[40]This section relies on the following key references: 1. Arthur, Winfred, et al. "Factors That Influence Skill Decay and Retention: A Quantitative Review and Analysis." *Human Performance* 11.1 (1998): 57-101; Perkins, GD, and ME Mancini. "Resuscitation training for healthcare workers."*Resuscitation* 80.8 (2009): 841-842.; Occupational Safety and Health Administration (OSHA), "Best Practices Guide: Fundamentals of a Workplace First Aid Program," http://www.osha.gov/Publications/OSHA3317first-aid.pdf.; Moser, D., 1992: Recommendations for improving cardiopulmonary resuscitation skills retention. In: Heart & Lung, 21:372-380.; Woollard, M., Whitfield, R., Newcombe, R., Colquhoun, M., Vetter, N., & Chamberlain, D. 2006: Optimal refresher training intervals for AED and CPR skills: A randomised controlled trial. In: Resuscitation,71: 237-247.; Ginzburg, S. & Dar-El, E., 2000: Skill retention and relearning – a proposed cyclical model. In: Journal of Workplace Learning, 12: 327-332.; Rose, A. M., Radtke, P. H., Shettel, H. H., & Hagman, J. D. (1985). User's manual for predicting military task retention (ARI Report No.85-26). Alexandria, VA: U. S. Army Research Institute for the Behavioral and Social Sciences.; and (DTIC No. ADA163710) Loftus, G. R. (1985). Evaluating forgetting curves. Journal of Experimental Psychology: Learning, Memory, & Cognition, 9, 730-746.

to reinforce proficiency and inform employees of any process changes. But understanding the precise amount of time it takes for specific skills to decline is a more complex problem, and no uniform measurement system currently exists for indexing retention.

In the case of CPR, a topic on which a significant number of studies exist, there is no across the board standard for certification length. Training providers like the American Red Cross require annual recertification, while other providers require certification every two years. The American Red Cross has reviewed 24 studies and found no evidence to support the claim that CPR skills are retained for two years. Though skill deterioration seems to plateau between year one and two, it is inadequate to respond to an emergency situation at year one. In order to counter CPR skill decay, experts recommend refresher courses every six months to provide opportunities to practice the techniques. The Occupational Safety and Health Administration (OSHA) released a document entitled "Best Practices Guide: Fundamentals of a Workplace First Aid Program," that encourages employers to lead review sessions for CPR and automated external defibrillators (AED) every six months, and recommends that staff be retrained annually.

While skill retention is a difficult concept to measure, it is clear that the rate at which skills and knowledge decay in an individual's memory is a function of the degree of original learning. Thus in order for training to be successfully retained, initial skill acquisition must be high and the newly learned proficiency must be effectively transferred into practice. Skills learned in a high acquisition environment (e.g. extensive training in a simulated environment) are retained longer than skills learned in a low acquisition environment (e.g. one-day seminar). Therefore it is equally important to measure skill acquisition, as it is to measure post-training performance.

Training records should be monitored to aid understanding of when refresher training is necessary to maintain the desired level of proficiency. Trainers can monitor reported and/or observed decrements in performance as criteria for measurement. For example, post-training performance evaluations are useful in order to understand the degree to which a skill has been lost. Trainers can also examine how the same task is performed under slightly different conditions, allowing them to gauge whether decay has occurred based on the original skill learned.

It follows that when considering a timeline for refresher training, three key issues should be addressed. First, how frequently is the skill practiced in the workplace? Second, how susceptible is that type of skill to decay? And finally, how much retraining is necessary to restore effectiveness? Addressing these questions is invaluable in order to keep employees optimally prepared, and also to save employers time and resources by identifying appropriate training intervals for the specific skill set.

There are a variety of biorisk skills relevant to laboratorians that may need different levels of refresher training. For example, working in a biological safety cabinet (BSC) is a fundamental skill utilized on a daily basis for containment laboratory work and for a lot of work in Biosafety Level 2 laboratories while cleaning up larger spills outside of a biological safety cabinet is also an important skill that ideally is never used. As noted, the length of time between skill acquisition and use is one key variable impacting skill retention. Use of a BSC is perhaps more comparable to a nurse giving shots while spill response may be more analogous to the CPR training needs described above. Applying the principles for refresher training to these two examples, clearly a high degree of initial learning is the ideal starting point and it is straightforward to develop training in a high acquisition format (hands on practical training) for both of these examples. But, the approaches to refresher training may differ substantively for these two skills. For example, the necessary BSC refresher training intervals might be determined by observations by biosafety professionals or laboratory managers. The "refresher training" might not need to be comprehensive either for BSCs but rather more narrowly focused on the observed lapses supplemented by annual review of key principles. The annual review of these BSC pointers could easily be accomplished through an online training module. In contrast, cleaning up spills outside of the BSC is important but ideally rarely used skill and it is a skill that is not a simply a discrete step of simple steps since spills can vary in magnitude and situation (e.g. spilling a 100 ml inside of *Brucella spp.* inside a centrifuge vs. spilling one liter of methicillin-resistant *Staphylococcus aureus* on the floor of the laboratory). Thus, based on the laboratory work, hands-on spill response training might need to be conducted more frequently. One possibility could be to ensure that at least one person inside a given laboratory has had the opportunity to practice their skills within the past 6 months.

Personnel Reliability Programs

> In looking for someone to hire, you look for three qualities: integrity, intelligence, and energy. But the most important is integrity, because if they don't have that, the other two qualities, intelligence and energy, are going to kill you. - Warren Buffet[41]

The effectiveness of any security system, no matter how technologically advanced, is ultimately determined by the training, reliability and integrity of the individuals who operate it. Within the confines of agents, materials and equipment that may be used destructively, the potentially catastrophic consequences of disloyalty, exploitation (blackmail) or a violent workplace incident make careful screening of the latter two characteristics imperative. Such vetting must be inclusive in scope. Originally established for chemical and nuclear weapons programs, the US Personnel Reliability Program (PRP) attempts to ensure that individuals are extremely reliable and exhibit supreme integrity. Typically PRP's are designed to achieve the highest possible standards of individual reliability in personnel

[41] Mary Buffet and David Clark, The Tao of Warren Buffet, 192 pgs, 2006.

performing duties associated with risk of misuse or with access to critical components. It is intended to prevent the unauthorized access, manipulation, theft, diversion, accidental or deliberate use of material or information. Unauthorized use may include nefarious purposes such as offensive use targeting crops, animals or humans, as sabotage, or for financial purposes.

Generally, PRPs pursue several lines of inquiry to develop a comprehensive picture of the individual in question. A background check is conducted to verify identity, credit history, criminal history, reputation and character. Psychological and medical screening are used to evaluate the mental health and stability of the individual; depression, schizophrenia, epilepsy, high/low blood pressure and other disorders are all taken into consideration. Additionally, a detailed interview to verify background information and elucidate other potential concerns is conducted at the time of employment or when a sensitive task is being assigned. Periodic reviews of job performance and coworker interaction are a standard means of ensuring that an employee's reliability remains high over time, and an individual's after work activities may also be monitored.[42] As an example, the following occurrences may result in decertification for nuclear duty: alcohol abuse/dependency, drug abuse, conviction of or involvement in a serious incident, an adverse medical—physical and mental—condition or serious progressive illness, lack of motivation, suicide attempt or threat.[43]

A PRP may be graded to reflect the varying level of sensitivity. Personnel in the PRP must be certified to a relevant industry standard.

Components and markers of a given PRP

Component	**Marker**
Trustworthy	Criminal History
Physically Competent	Medical Evaluation
Mentally Competent	Mental Health History
Emotionally Stable	Psychological Evaluation
Financially Stable	Credit History
Responsible to uphold obligations to safety, public health, national security and scientific integrity	Drug Testing, Peer Review, Affiliations

[42]Basrur Rajesh M. and Hasan-Askari Rizvi. "Nuclear Terrorism and South Asia." Cooperative Monitoring Center Occasional Paper/25. Sandia National Laboratories. Feb. 2003. http://www.cmc.sandia.gov/Links/about/papers/occasional-papers/nuclear-terrorism-op25.pdf

[43] Basrur Rajesh M. and Hasan-Askari Rizvi. "Nuclear Terrorism and South Asia." Cooperative Monitoring Center Occasional Paper/25. Sandia National Laboratories. Feb. 2003. http://www.cmc.sandia.gov/Links/about/papers/occasional-papers/nuclear-terrorism-op25.pdf

While all entities of the US Federal Government have some form of PRP[44], other areas of business in the US, whether private or public, may not have PRPs in place. Also, the norms and requirements likely vary internationally. An example in the biosecurity arena is given below, in which the requirements in the US are compared to those of Denmark. Finally, the standards of PRPs differ across industries, as explained in further detail below. This probably reflects differences in risks (real or perceived), e.g. securing economic assets as opposed to securing items of potential offensive nature. In addition, historic developments and cultural traits may serve as influencing factors.

The field of biology

In a biosecurity framework, a PRP is part of the overall protective posture, and supplements safety and security measures. The principal objective of personnel security programs and personnel reliability programs in bioscience institutes is to protect members of the scientific, public health, veterinary, and medical communities. There is currently little, if any, evidence on the potential impact of PRP programs on whether they would deter a qualified scientist from pursuing important research. Ideally, they would, if implemented properly, serve to protect the integrity of research programs and affiliated personnel. As part of a web of prevention, the PRP specifically targets the threat from insiders. An insider is usually an employee who is privy to, not simply facts and procedures, but also the day-to-day working relationships and dynamics of people in the specific workplace.

The relationship of personnel reliability with safety, security and material control and accountability (MC&A) may be outlined as below:

Framework	**Examples**	**Counters**
Safety	Health protection Equipment controls Guidelines/practices Medical screening	Accidental release
Security	Physical protection Access controls Guns, guards & gates Visitor screening	Outsider threat
Personnel reliability	Institute protection Researcher controls Routine monitoring Personnel screening	Insider threat
MC&A	Item integrity Purpose Accountable person – qualified, authorized and able	Insider threat

[44]Presentation by Jay Frerotte, Director Environmental Health & Safety, Responsible Official for Select Agents, University of Pittsburgh, "Personnel Reliability Programs," CSHEMA 2009, New Orleans.

The recent report[45] in May 2009 from the National Science Advisory Board for Biosecurity (NSABB) concluded that the Select Agent Program has been fortified since 2001 to address personnel reliability, institutions effectively screen individuals, that there is very little evidence that PRPs have predictive value for criminal activity, and that engaged institutional leadership can mitigate the risk of an insider threat. The recommendations suggested that the culture of responsibility and accountability should be enhanced at institutions rather than enforcing a mandated PRP, that professional societies should continue to encourage dialogue about biosecurity, and that the list of Select Agents should be modified. These findings were formally supported by the American Biological Safety Association (ABSA), and further maintained by the May 29, 2009 Report of the American Association for the Advancement of Science (AAAS) titled Biological Safety Training Programs as a Component of Personnel Responsibility.[46]

Clearly there is a discourse between conservationists (exemplified by ABSA, NSABB and AAAS) that advocate that current regulation is sufficient or even too burdensome, and proponents of introducing additional, perhaps more prescriptive, measures that mimic those in the nuclear field (see below). The latter are often promoted by individuals or agencies dealing with traditional physical security, but without sufficient insight into the professional requirements and daily operations of a bioscience facility.

Thus, in an effort to inform this debate, the following section of this report reviews the PRP standards in other relevant industries. As outlined, many industries employ some level or aspect of personnel reliability and many industry standards exceed those used in the select agent community. On a related note, the notion of a license to practice life science research is a relatively new idea that has not been debated publicly. A criticism of the Select Agent Regulation is that individual security risk assessments (personnel screening) are not portable, making it difficult for investigators to work in multiple locations (sometimes a key component of collaboration). A licensure framework could address this. Further, state licensure is required of nearly every aspect of the US health care profession in order to protect the community from the health risks of malpractice; some research institutes carry out an extensive credentialing process. Active management of laboratory personnel, encompassing regular performance evaluations, ongoing training, and clear mechanisms for reporting concerns is also vital for ensuring personnel reliability.

---

[45] NSABB, Enhancing Personnel Reliability among Individuals with Access to Select Agents, May 2009.
http://oba.od.nih.gov/biosecurity/meetings/200905T/NSABB%20Final%20Report%20on%20PR%205-29-09.pdf

[46] AAAS Center for Science, Technology and Security Policy and AAAS Program on Scientific Freedom, Responsibility and Law, Biological Safety Training Programs as a Component of Personnel Reliability, Workshop Report, 2009.

A comparative analysis of the US and Danish biosecurity laws and regulations[47], highlighting differences in the two approaches, illustrated that PRP requirements are among the most diverging aspects. The US Select Agent Program[48] focuses on 8 areas as part of the PRP to ensure that restricted and prohibited persons as defined by the USA PATRIOT Act are not granted access to select agents.

- Criminal record
- Illegal drug use
- Unlawfully in the US
- Adjudicated mentally defective
- Foreign national of State sponsor of terrorism
- Dishonorable discharge from the military
- Terrorism involvement
- Foreign agent

This applies to the executive management, the responsible officer and people with access to Select Agents. In contrast, the Danish regulations on PRP only focus on the criminal record, and this applies only to the responsible officer.[49] This comparative analysis showed that even within the bio-community there are markedly different approaches to the issue of PRP. As pointed out earlier, this may be due to differences in cultures and social norms.

The US Army also has its own Biological Personnel Reliability Program (BPRP).[50] There are currently over 600 enrollees in the Army BPRP. The existing chemical surety program[51] was used as a basis for the biological surety program and BPRP.
The Army BPRP qualifying standards include:

- Mentally alert, stable, trustworthy, physically competent, free of unstable medical conditions
- Dependable, responsible, perform in approved manner
- Flexibility in adjusting to changes in working environment
- Good social adjustment
- Sound judgment in adverse or emergency situations
- Physical ability to perform required duties
- Positive attitude towards the BPRP

BPRP mandatory disqualifying standards include:

- Current diagnosis of drug/substance or alcohol dependence
- Drug/substance abuse within 5 years of initial interview
- Drug trafficking within 15 years of initial interview
- Drug/substance abuse while enrolled in the PRP
- Inability to meet safety requirements of the position

Other disqualification factors (certifying official judgment required):

---

[47] J. Gaudioso and E. Heegaard, Comparative Analysis of US and Danish Biosecurity Regulatory Approaches, poster presentation, European Biosafety Association Conference, Stockholm, Sweden, June 2009.
[48] www.selectagents.gov
[49] Danish Law 69, June 12, 2008.
[50] Army Regulation 50-1, Biological Surety
[51] Army Regulation 50-6, Chemical Surety

- Alcohol-related incidents/alcohol abuse
- Drug/substance abuse more than 5 years before initial interview
- Medical conditions or treatment that: affect consciousness, judgment, concentration, impair ability to wear
- protective equipment, or impair physical ability required for duties
- Suicide attempts or threats
- Inappropriate attitude, conduct, or behavior, including concealing or failing to report potentially disqualifying information

The field of nuclear science and weapons

In the US, the nuclear PRP[52] is a set of psychological tests and organizational checks tailored to specific DOD requirements; DOE has a similar program under a different name. PRP's are viewed as a primary means of countering the insider threat. The basic theory supporting this judgment is that a financially insolvent, disgruntled or mentally unstable insider can carry out theft or sabotage (alone, or with the help of outsiders), and thus should not be allowed access to nuclear weapons or materials.

The US nuclear PRP began in the 1960's and screens military, civilian and contractor personnel whose duties give them access to nuclear weapons, components of nuclear weapons, or the codes, computer tapes and communications equipment used to launch them. As noted, abuse of alcohol, drugs, or the identification of emotional problems may result in decertification.[53]

DOD PRP policy is developed and implemented by the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD C3I). The Assistant Secretary of Defense for Force Management and Personnel advises the ASD C3I, as does the ASD for Health Affairs and the DOD General Counsel.[54] U.S. military bases/units are rated on their overall PRP performance. A unit PRP monitor becomes a liaison to the unit commander to keep him abreast of PRP developments and unit deficiencies. The PRP monitor also conducts briefings for officers and enlisted personnel on PRP guidelines, checklists, etc.[55]

---

[52]AFI 36-2104, Nuclear Weapons Personnel Reliability Program, May 29, 2003; AFI 31-501, Personnel Security Program Management, August 1, 2000; AFI 91-101, Air Force Nuclear Weapons Surety Program, February 24 2000

[53] Norris, Robert S. and William M. Arkin. Eds. "Nuclear Notebook: Bombed Out." Bulletin of the Atomic Scientists. Vol. 44, No. 6 (July 1988): pp. 23.

[54] United States Department of Defense Regulation Number 5210.42. Nuclear Weapon Personnel Reliability Program. January 8, 2001. http://www.dtic.mil/whs/directives/corres/text/d521042p.txt

[55]Godbey, Kelly. "Personnel Reliability Program." The Inspector General Brief. Vol. 53, No. 5 (Sep/Oct. 2001): 16-17. http://afia.kirtland.af.mil/TIG_PUBLIC/library/Word/2001/Sep-Oct%2001%20TIG%20Brief%20for%20Word.doc,

Initially, top level background investigations and, in some cases, polygraphs are used to screen and rescreen individuals for the DOD PRP program.[56] Additionally, an integrated inspection and assessment process ensures that guidelines are being followed throughout the program.[57] The original screening process is augmented by continuous evaluation, and the program encourages self-reporting for individuals to remove themselves from nuclear-related duties if problems arise. Suspension of certification is non-punitive and occurs independently of disciplinary action.[58] The failure of an individual to be certified for nuclear-related duty does not reflect on that individual's ability to perform other duties.[59]

In 1990, there were approximately 66,500 persons, including 1,800 civilians, enrolled in DOD's PRP program. However, this number has decreased in proportion to the subsequent cutbacks in nuclear weapons programs.
Commercial nuclear reactor workers in the U.S. are subject to similar checks, which include background checks, random drug and alcohol screenings and other security management programs. One such program is the Continuous Behavior Observation Program, which works to ensure that supervisors and colleagues will report suspicious behavior of any individual.[60]

The effectiveness of US PRP programs has been called into question several times, both for its structure and implementation. The DOD PRP is not without problems. At least one study has documented "significant levels of psychiatric disorders and drug and alcohol abuse, as well as of actual violent acts by military personnel cleared through personnel reliability screening programs" in the US.[61] For example, in a one-year period from January 1989 to January 1990, four PRP-certified personnel at one DOD facility committed suicide and or multiple murders.[62] Clearly then, although the U.S. PRP program and its DOE analogs are probably the most detailed and comprehensive screening programs in the world, care must be taken to ensure both that the programs are designed effectively and that they are implemented as they were intended. For example, in a 1992 report, the GAO argues

---

[56] Wells, Linton II (Principal Deputy Assistant Secretary of Defense Command, Control, Communications and Intelligence). Testimony before the Strategic Subcommittee of Senate Armed Services Committee. December 13, 2001.
[57] Wells, Linton II (Principal Deputy Assistant Secretary of Defense Command, Control, Communications and Intelligence). Testimony before the Strategic Subcommittee of Senate Armed Services Committee. December 13, 2001.
[58] United States General Accounting Office. "Nuclear Personnel Reliability Program." GAO/NSIAD-92-193R. May, 1992.
[59] United States Department of Defense Regulation Number 5210.42. Nuclear Weapon Personnel Reliability Program. January 8, 2001.
[60] Sagan, Scott D. "The Problem of Redundancy Problem: Why More Nuclear Security Forces May Produce Less Nuclear Security." Center for International Security and Cooperation. Stanford University. 2003.
[61] Basrur Rajesh M. and Hasan-Askari Rizvi. "Nuclear Terrorism and South Asia." Cooperative Monitoring Center Occasional Paper/25. Sandia National Laboratories. Feb. 2003. http://www.cmc.sandia.gov/Links/about/papers/occasional-papers/nuclear-terrorism-op25.pdf
[62] Abrams, Herbert L. "Human Reliability and Safety in the Handling of Nuclear Weapons." Science and Global Security. Vol. 2 (1991): 325-349. http://www.princeton.edu/%7Eglobsec/publications/pdf/2_4Abrams.pdf

that efforts to increase the frequency of peer reporting should be undertaken with vigor. This method of gathering information is seen as highly valuable, yet grossly under-utilized due to people's inherent reluctance to report on their friends and associates.[63]

Specifically, the US DOD has set up a PRP as a psychological evaluation program, designed to permit only the most trustworthy individuals to have access to nuclear weapons. The program was first instituted during the Cold War. Among its goals are:[64]

> 1. The Department of Defense shall support the national security of the United States by maintaining an effective nuclear deterrent while protecting the public health, safety, and environment. For that reason, nuclear-weapons require special consideration because of their policy implications and military importance, their destructive power, and the political consequences of an accident or an unauthorized act. The safety, security, control, and effectiveness of nuclear weapons are of paramount importance to the security of the United States.
>
> 2. Nuclear weapons shall not be subject to loss, theft, sabotage, unauthorized use, unauthorized destruction, unauthorized disablement, jettison, or accidental damage.
>
> 3. Only those personnel who have demonstrated the highest degree of individual reliability for allegiance, trustworthiness, conduct, behavior, and responsibility shall be allowed to perform duties associated with nuclear weapons, and they shall be continuously evaluated for adherence to PRP standards.

The PRP program evaluates many aspects of the individual's work life and home life. Any disruption of these, or severe deviation from an established norm would be cause to deny access. The denial might be temporary or permanent. However, the policy does explicitly state:

> The denial of eligibility or the revocation of certification for assignment to PRP positions is neither a punitive measure nor the basis for disciplinary action. The failure of an individual to be certified for assignment to PRP duties does not necessarily reflect unfavorably on the individual's suitability for assignment to other duties.

The investigative requirements for the PRP are based upon the sensitivity of the position. Positions in the PRP are designated as either critical or controlled.

<u>Responsibilities</u>

- Wing commanders are responsible for the wing PRP. They serve as the reviewing official for all permanent decertification case files started by

[63] United States General Accounting Office. "Nuclear Personnel Reliability Program." GAO/NSIAD-92-193R. May, 1992.
[64] DOD Directive 5210.42

subordinate units. They also approve or disapprove requests for removal or permanent decertification for subordinate units

- Group and unit commanders who control nuclear weapons, weapon systems, or critical components, are certifying officials (COs) who certify and initiate decertification for their personnel. They may delegate this duty to a deputy or assistant. Certifying officials and their delegates must be certified in a PRP category equal to, or higher than the personnel they are certifying
- Individuals in the PRP must monitor their own reliability. They must also notify the CO of any potentially disqualifying information (PDI) (either their own or that of co-workers)

Categories of PRP positions

- Critical position: requires a person to be in close physical proximity to a nuclear weapon. This person controls access to or uses technical data on the electrical or mechanical parts, or has access to unlock and or authenticate values of a nuclear weapon or weapons system that launch, release, or detonate the weapon
- Controlled position: requires the assigned person to enter a "no-lone" zone or to control entry into a "no-lone" zone. This person has access, but no technical knowledge pertaining to the launching, releasing, or detonating of a nuclear weapon or critical component

PRP mandatory selection criteria

Individuals selected and certified for the PRP must meet the following minimum criteria at all times

- Have an S-1 (no psychiatric disorder) profile (or civilian equivalent)
- Are technically competent
- Have the required security investigation and security clearance
- Have a positive attitude toward nuclear weapons duty and the PRP objectives
- Are not under consideration for separation for cause, under court-martial charges, or awaiting civilian trial for felony or misdemeanor charges
- Are US citizens or US nationals

Certifications

- A formal certification occurs when an individual is placed in PRP and possesses the required security investigation
- An interim certification occurs when an individual is placed in PRP and does not possess the required security investigation for formal certification, but does have a security investigation adequate for interim clearance
- An administrative certification is granted when an individual is not currently formally or interim certified for PRP duties and is identified for an assignment to a PRP position

Removal from PRP

Members may be removed from PRP duties in one of three ways: by suspension, by temporary decertification, or by permanent decertification

Suspension

- Suspension is used to immediately remove an individual from PRP-related duties (for a maximum of 30 days) without decertification
- The individual is still considered reliable with regard to the PRP, but because of the circumstances, cannot perform the nuclear related duties requiring PRP certification. The certifying official can use this time to research the facts to determine if an individual's reliability is impaired. However, a suspension should not be used in place of decertification when the facts and circumstances indicate unreliable behavior
- The certifying official makes the final decision

Temporary Decertification

- Temporary decertification is used to keep an individual from performing nuclear related duties for up to 180 days when an individual's job performance or reliability is in question or impaired and neither suspension nor permanent decertification is appropriate. The temporary decertification may be extended in 30-day increments up to 270 days if more time is needed to make a decision
- A temporary decertification should not be used in place of a permanent decertification if the facts indicate a permanent decertification is more appropriate

Permanent Decertification

- Permanent decertifications are used to remove an individual from the PRP in situations that will not allow for suspension or temporary decertification. Permanent decertification indicates the individual has questionable reliability or long-term impaired capability.
- Permanent decertification is appropriate when
    - The individual's drug abuse has been confirmed
    - The individual is diagnosed as an alcohol dependent
    - The individual is being involuntarily discharged or removed for cause
    - The individual no longer meets the mandatory selection criteria (see list of criteria above)
    - The individual is not qualified for administrative certification for PCS or training; or
    - The individual's security clearance eligibility has been revoked

The field of chemistry

The US Military has developed procedures for the Chemical Personnel Reliability Program (CPRP)[65] personnel and related responsibilities. These procedures are applicable to all personnel involved in the accomplishment of CPRP related duties.

[65] Army Regulation 50-6, "Chemical Surety."

Applicants are screened for citizenship, security clearance, and suitability information.

- Citizenship: If the candidate is not a US Citizen, screening terminates at this point.
- Security Clearance: Determine the level of security clearance, date clearance granted, type of investigation, and date investigation completed on the selectee. The clearance information must meet the requirements of AR 50-6.
- Suitability: An official representative will review for Personal Disqualifying Information (PDI), the candidate's OPF, appraisal files, suitability files and any other appropriate files maintained. Examples of PDI are contained in AR 50-6.

Candidates are then grouped based on suitability determinations, not unlike the nuclear standards. The procedures incorporate continued evaluation, maintenance of licenses and administrative termination.

Financial

The financial sector includes a diverse set of employees and responsibilities, covering anyone who comes into physical contact with money or electronic access to or transferring of funds, etc. Examples of the former include clerks in banks, money transportation staff (e.g. crews of armored vehicles), and people otherwise processing money or producing bank notes and coins. The latter group comprises accountants, managers and executives among others. Serving as an example European financial executives will be examined in some detail in this subsection.

Throughout Europe the reliability requirement for financial executives is largely based on European Commission law, which requires managers of credit institutions, insurance companies and the like to be of good repute.[66] This requirement is found in a considerable number of directives, the most prevalent of which is the Markets in Financial Instruments Directive (MiFid), which concerns investment firms and regulated markets.[67] MiFid holds that when the requirements under which authorization was granted are no longer met, the authorization may be withdrawn. To ensure compliance with the MiFid, the Member States must designate the authorities which are to carry out the duties provided for in the directive (Article 48(1)). To execute their tasks, the competent authorities must at least have powers pertaining to access to relevant information, the power to require the cessation of any practice that is contrary to the provisions adopted in the implementation of the directive (Article 50(2)(e)), and the power to adopt any type of measure to ensure that investment firms and regulated markets continue to comply with legal requirements. Despite the importance of the requirement, the criteria one must meet to be deemed of sufficiently good repute are lacking in most

[66] Anoeska Buijze, http://www.utrechtlawreview.org/ Volume 4, Issue 3 (December) 2008.
[67] Directive 2004/39/EC of 21 April 2004 on markets in financial instruments (MiFid).

of these directives. Where they can be found, they require no previous bankruptcy and a clean criminal record with regard to relevant offenses.[68]

The Committee of European Securities Regulators (CESR) clarified the good repute requirement found in the Investment Services Directive (ISD) in its European standards on fitness and propriety to provide investment services.[69] Accordingly, the fit and proper criterion requires persons 'to meet high standards of personal integrity in all respects and to be competent and capable of performing the functions or role currently performed or which it is proposed they should perform in the firm'. To evaluate whether this requirement is met, a minimum standard of what information should be considered, including personal details, education and qualifications and a complete work history. Of particular relevance for the assessment of reliability are someone's criminal record and information about any previous civil cases, including disqualification as a company director or bankruptcy. The competent authorities can opt to exclude certain types of offenses, such as motor vehicle violations. For the evaluation of someone's personal financial integrity, the authorities can check current and past personal solvency. Providing inaccurate or misleading information can be a reason to fail the fit and proper test, but apart from that the standards give no guidance as to when the authorities should conclude, based on the relevant information, that an individual does not meet the standards.

For comparison, in Germany the reliability criterion is a general requirement in German trade law.[70] Anyone who practices a trade in the sense of the Industrial Code needs to be sufficiently reliable to execute that trade. If any kind of authorization is required to practice the trade, this can be refused when reliability is lacking. Reliability is defined in a negative way: it is lacking when the subject, based on his personality, does not offer the guarantee that he will practice his trade according to the rules. The judgment is connected to a specific position. Therefore, any facts that show unreliability can only be taken into account when they show unfitness for this particular position, and reliability must be judged in the context of the application for authorization that gave rise to the test. Prior convictions, especially for crimes against property, fraud, tax transgressions and forgery will weigh heavier on someone's record than other crimes. The closer the crime is connected to the executive's position, the heavier it weighs on his reliability. Personal weaknesses and flaws can only be considered if they have an effect on the functioning of the individual in his capacity as an executive.[71]

There are many functions outside the financial realm for which there is a reliability criterion, and more often than not this criterion is based on European Commission law. In some parts of Europe, to meet this criterion, one has to be able to show a

[6868] Anoeska Buijze, http://www.utrechtlawreview.org/ Volume 4, Issue 3 (December) 2008.
[69] Directive 93/22/EC of 10 May 1993, *OJ* L 145, 30.4.2004.
[70] M. Schüler, *Integrated Financial Supervision in Germany*, 2004, Discussion paper no. 04-35 of the Zentrum für Europäische Wirtschaftsforschung GmbH.
[71] Anoeska Buijze, http://www.utrechtlawreview.org/ Volume 4, Issue 3 (December) 2008.

Certificate of Good Conduct.[72] To acquire such a certificate, one has to send an application to the mayor of the town where one lives, who will send the request to the relevant Minister. It is the mayor's responsibility to check whether the information the applicant has supplied is correct, and he can advise the Minister on any special circumstances in his municipality that might affect the decision. The Minister will decide on the request, taking into consideration the risk for society in relation to the purpose for which the certificate has been requested and the interest of the applicant. A certificate is refused when there is a criminal antecedent in the criminal records, which, considering the risk posed to society, if repeated, will harm the proper execution of the task for which the certificate was requested. If the criminal records do not contain any data on the applicant for the past four years, the certificate will be issued, unless the applicant has been found guilty of a sexual offense, in which case there is no time-limit, or has been imprisoned at anytime in the past four years.[73]

Health care

The integrity of health care workers is obviously of concern. This work involves being entrusted with sensitive information, and sharing of results across many sectors mainly within the health services. Also, ensuring required levels of training, expertise and skills are important. The interactions often involve personnel that one may have no personal experience with, necessitating a uniform minimum standard, which may be met through portable licensing, continued educational programs, etc. Staff support programs directed at alcohol and drug abuse exist, but do not differ from what is widely available. The unique aspect of the medical profession is the availability of drugs; a concern which is controlled in different ways.

Institutionalized PRPs in the health sector were not identified. As an example, when conducting an interview with The Danish National Board of Health, it became clear that there are no restrictions in terms of criminal records. The National Board of Health may revoke licenses based on poor professional performance. The requirements are strictly based on professional skills. The relevant professional society may disbar members based on a specific assessment, which most likely would require being convicted for a major felony such as murder, lethal arson or serious sexual misconduct involving minors.

Aviation industry

Physical security is graded at the airport, in which crew members undergo a more rigorous control, as opposed to ground staff. Formal licensing of crew members provides some level of assurance on performance standards, identification and access, but does not directly address personnel reliability. Interviews conducted with a couple of representatives from the airline industry in Denmark indicate that only rudimentary aspects of personnel reliability come into play in the Scandinavian Airlines System and Thomas Cook. For crew members, the criminal record must show no misdemeanors in the past 5 years. In addition, driving under

[72] Art. 30(1) Judicial Data and Criminal Records Act, NL
[73] Anoeska Buijze, http://www.utrechtlawreview.org/ Volume 4, Issue 3 (December) 2008.

the influence (DUI) does not automatically affect licensing. The same rules apply in Norway, while Sweden apparently does not require a clean criminal record when issuing a pilot certificate. Indirectly, the pilots face slightly more stringent demands, due to the fact that they on a regular basis (previously semi-annually, now annually) undergo a physical examination. This includes testing liver enzymes, which may offer circumstantial evidence of an elevated intake of alcohol. However, this is merely indicative, and is not evidence of being intoxicated at the workplace. These visits are announced and it is apparently well recognized that pilots being tested right after a being on vacation exhibit elevated levels of liver enzymes. There is no formal random or fixed drug testing in place. Likewise, alcohol testing is seemingly very uncommon, to the extent that it may never be used. Others point to the fact that for the past year random alcohol testing has been established. Anecdotally, crew members have been barred from work due to suspected alcohol abuse. A whistle-blower system is supposedly not in place, or receives little attention, and a formal behavioral assessment program could not be identified.

The International Air Transport Association (IATA) has developed the commercial standards of the global aviation industry. IATA has more than 230 airline members, representing 93 percent of scheduled international air traffic. Complying with international regulations, IATA has set up guidelines regarding the safe and secure transportation of goods. However, it is not clear if IATA-endorsed PRP's exist.

Crew members serving international destinations occasionally have to comply with more stringent background checks. Apparently, US Federal Regulations requires additional information regarding the crew members on flights coming to the US, which is covered by issuing a special visa. This specifically involves a visit at the local US Embassy in order to be cleared for commercial flights. The specifics of the approval process are unclear. Most likely it is a unilateral national approach, as has been the case with US requirements regarding advance notice on passenger names. Piloting in and out of the US on a private non-commercial basis does not come under these regulations. Supposedly anyone with a certificate can fly all over the world privately.

New rules are being introduced by the European Union regarding certificates. Apparently, Joint Aviation Requirements (JAR) exist, and this will likely influence the way that certificates are produced.[74] Supposedly guarding from fraud and making the appearance more uniform. Currently, the value of a PRP is undercut to a certain extent by the fact that certificates are extremely easy to forge (no photo, no personal unique identifying number etc). A certificate combined with a proper uniform will provide rather easy access (the industry has some stories testifying this).

[74] http://www.jaa.nl/publications/publications.html#

What does this mean for biosecurity PRPs?

There is likely a pattern in how to guard economic assets (Finance) or providing general security (Aviation) as opposed to granting access to materials and equipment that traditionally has clear and destructive potential (Arms). Albeit, these traditional sectors are undergoing changes that will likely increase the general level of security, which may or may not influence the future role of PRPs more broadly. It is currently not clear how best to approach personal reliability issues in biosecurity, as the biosciences does not mirror existing industries. The challenge involves striking a balance between the legitimate use and the potential for misapplication. This is perhaps not unique for biology, but in no other setting is the challenge this marked, and the distinctions so subtle.

Equally, a global understanding of PRPs remains incomplete. For example, information regarding the PRPs of other nuclear powers is extremely limited both because of classification issues and a lack of concern about the security of their nuclear arsenals.[75] As of 1991, France conducted PRP-like screening of its nuclear personnel and ensured that primarily senior officers were assigned to nuclear duty. In contrast, Britain did not employ any special screening of nuclear personnel beyond the usual check in fitness for military service.[76] As of 1991, China had no PRP program in place beyond a check of an individual's political background. However, drug and alcohol abuse do not appear to be a serious problem in China.

Personnel reliability programs are an essential piece of any security regime. If the integrity and stability of those with access to materials is not assured, the most rigorous physical security is vulnerable to sabotage or circumvention. Available evidence suggests that "perfect" PRPs do not exist, and that serious deficiencies abound even in traditional nuclear PRP areas. Ultimately, PRPs are not foolproof, thus society must always accept some level of risk from the insider.

The ambiguous picture painted by sparse evidence suggests that further study of PRPs in different industries is warranted, before settling on the best practice approach and level of a biosecurity PRP.

MANAGEMENT SYSTEM APPROACHES FOR EFFECTIVE RISK GOVERNANCE

Managing laboratory biorisks is a complex, multivariate problem, involving many interrelated processes. There are many other fields that must similarly tackle challenges to work safely and securely with hazards, such as the chemicals, aerospace industry, and mining. Management systems are designed to address such problems. Common management systems include ISO 9000, a quality management system to help organizations continually improve the quality of their product, customer service, and productivity; ISO 14000, an environmental management

[75] Ryan Crow, Personnel Reliability Programs, Project Performance Cooperation, 2004

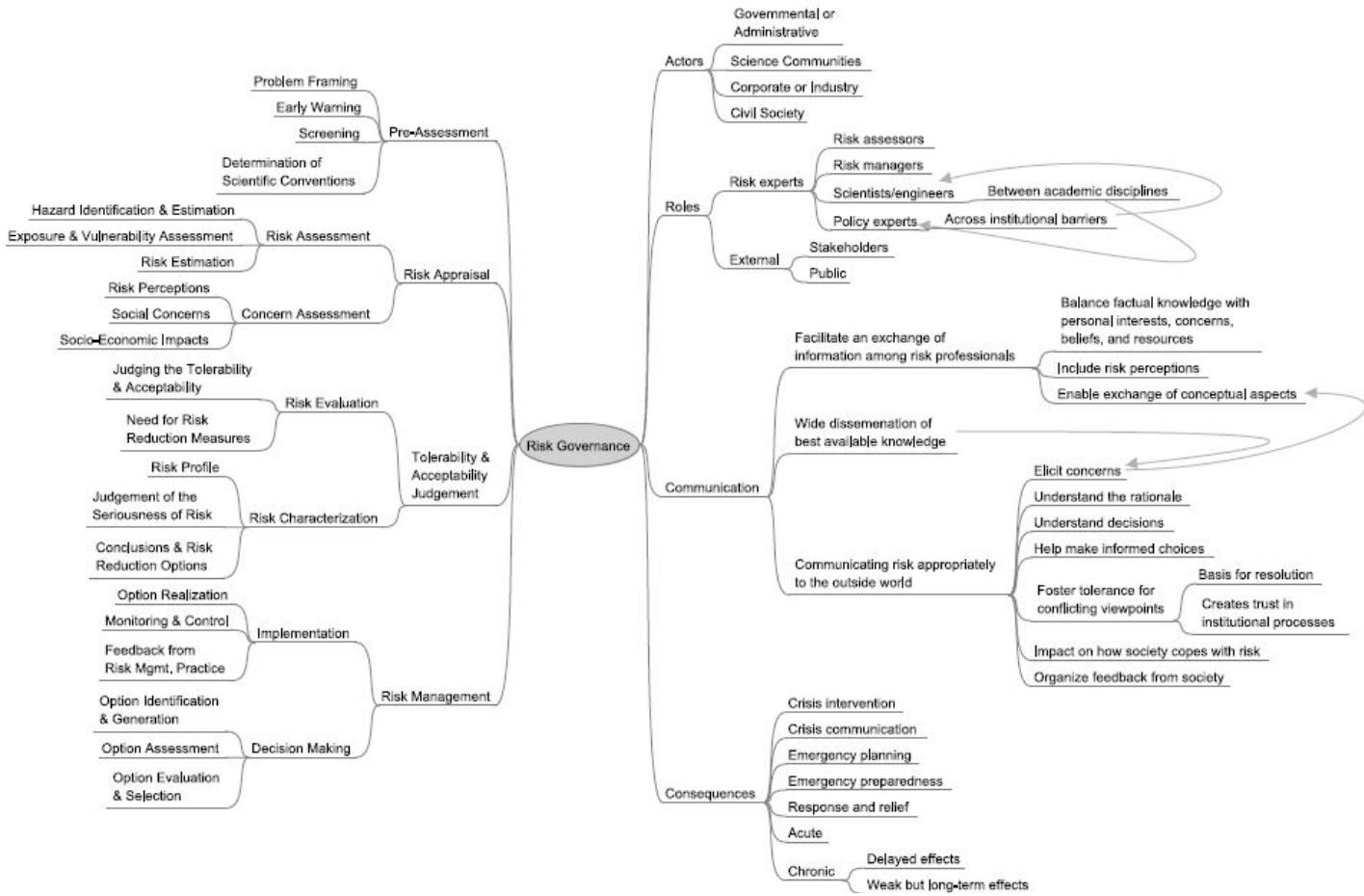
[76] Abrams, Herbert L. "Human Reliability and Safety in the Handling of Nuclear Weapons." Science and Global Security. Vol. 2 (1991): 325-349

system to help organizations conduct their work in a way that minimizes impact on the environment and continually improves their environmental performance; and OHSAS 18000, an occupational health and safety management system to help organizations continually improve health and safety within their activities. Recognizing the uniqueness of laboratory biorisks, the CWA Laboratory Biorisk Management Standard is a management system approach to enable an organization to effectively identify, monitor, and control the laboratory biosafety and biosecurity aspects of its activities.[77] This is a new standard and, as laboratories begin to implement it, there may be useful lessons learned from the implementation of other management systems to determine how such a system is implemented effectively. An effective management system approach should be built on the concept of continual improvement through a cycle of planning, implementing, reviewing, and improving processes that an organization takes to meet goals. In order to review and improve processes, performance indicators need to be defined for the organization's system. This is one of the major challenges to effective implementation of any biorisk management system.

Institutions that manage biorisk according to a management system approach are usually confronted by the limitations for checking of the biorisk management performance: the lack of suitable monitoring tools. In most settings, incidents and accidents involving biological agents or materials are very rare (even though they could have major consequences should they occur), so incident rates, which are a classical performance indicator in general safety, do not have any statistic significance when applied to biorisk. In many places, the reporting of small incidents without consequences, or near-misses (such as minor spills and small injuries without direct exposure), is not required or not effective. The best performance indicators should not only be quantifiable and usable as monitoring tools on a dashboard, but should also provide a way to evaluate the management program in a more qualitative way in order to define what needs to be improved. There is clearly a need to identify and develop ways to reach these objectives in assessing the performance of biorisk management.

Understanding all of the elements relevant to a biorisk management system is the first step to being able to develop suitable performance indicators. The figure below is a mind map, showing the relevant elements and their interrelations, demonstrating the complex, multivariate nature of laboratory biorisk management.

[77] "Laboratory biorisk management standard", CWA 15793:2008 (ftp://ftp.cenorm.be/PUBLIC/CWAs/wokrshop31/CWA15793.pdf).


Risk Governance
Pre-Assessment
Problem Framing
Early Warning
Screening
Determination of Scientific Conventions
Risk Appraisal
Risk Assessment
Hazard Identification & Estimation
Exposure & Vulnerability Assessment
Risk Estimation
Concern Assessment
Risk Perceptions
Social Concerns
Socio-Economic Impacts
Tolerability & Acceptability Judgement
Risk Evaluation
Judging the Tolerability & Acceptability
Need for Risk Reduction Measures
Risk Characterization
Risk Profile
Judgement of the Seriousness of Risk
Conclusions & Risk Reduction Options
Risk Management
Implementation
Option Realization
Monitoring & Control
Feedback from Risk Mgmt. Practice
Decision Making
Option Identification & Generation
Option Assessment
Option Evaluation & Selection
Actors
Governmental or Administrative
Science Communities
Corporate or Industry
Civil Society
Roles
Risk experts
Risk assessors
Risk managers
Scientists/engineers
Between academic disciplines
Policy experts
Across institutional barriers
External
Stakeholders
Public
Communication
Facilitate an exchange of information among risk professionals
Balance factual knowledge with personal interests, concerns, beliefs, and resources
Include risk perceptions
Enable exchange of conceptual aspects
Wide dissemenation of best available knowledge
Communicating risk appropriately to the outside world
Elicit concerns
Understand the rationale
Understand decisions
Help make informed choices
Foster tolerance for conflicting viewpoints
Basis for resolution
Creates trust in institutional processes
Impact on how society copes with risk
Organize feedback from society
Consequences
Crisis intervention
Crisis communication
Emergency planning
Emergency preparedness
Response and relief
Acute
Chronic
Delayed effects
Weak but long-term effects

Biorisk Dashboard

This section explores the approaches and challenges to developing performance indicators for other safety management systems that have been put into place in many different industries around the world. We believe many of the ideas outlined in this section warrant further consideration and validation for their use in biorisk management systems. Although the research for this section relied on the extensive literature in the field of 'safety science,' most of the concepts are easily extended to address biosecurity concerns also. Additional work is needed to develop these concepts into a harmonized approach for creating a Biorisk Dashboard to monitor the performance of biorisk management systems.

Historically, safety programs have relied on accident and incident data to evaluate their effectiveness.[78] However, Glendon and McKenna[79] identify 15 reasons why accident data or similar outcome data are poor measures of safety performance. Traditional measures of safety are "after-the-fact" measures. Focusing on these measures (e.g., accident rates and compensation costs) means that the success of safety is measured by levels of system failure.[80] The recent safety literature is replete with examples where the traditional approach to safe work practices, revolving around employee training and enforcement of safety rules and regulations, has yielded suboptimal results.[81] Many modern approaches advocate the use of proactive measures (e.g., safety climate, hazard identification and /or observed percent safe behavior) that focus on current safety activities to ascertain system success rather than system failure. In combination, both approaches can help organizations to ascertain the effects of their safety programs.[82]

Ideally, at least two independent measures are used to assess performance or to gauge program effectiveness.[83] The purpose of indicators is to become tools, to be used as input values in the context of the management system. Because of the complex nature of safety and security, which involves external as well as internal and both intangible factors and measurable parameters, there are many aspects which cannot be expressed through objective, easily measurable indicators. Indicators are observable measures that should meet the following criteria:[84]

---

[78] Flin, R., Mearns, K., O'Connor, P., & Bryden, R. (2000). Measuring safety climate: identify the common features. *Safety Science , 34*, 177-192.

[79] Glendon, AI, EF McKenna, (1995). Human safety and risk management. London: Chapman and Hall.

[80] Choudry, R. M., Fang, D., & Mohamed, S. (2007). Developing a Model of Construction Safety Culture. *Journal of Management in Engineering , 23* (4), 207-212.

[81] DeJoy, D. M., Gershon, R. R., & Schaffer, B. S. (2004, July). Safety Climate: Assessing management and organizational influences on safety. *Professional Safety* , 50-57.

[82] Cooper, M., & Phillips, R. (2004). Exploratory analysis of the safety climate and safety behavior relationship. *Journal of Safety Research , 35*, 497-512.

[83] Glendon, A., & Litherland, D. (2001). Safety climate factors, groups differences and safety behaviour in road construction. *39*, 157-188.

[84] Jovasevic-Stojanovic, M., & Stonjanovic, B. (2009). Performance Indicators for Monitoring Safety Management Systems in Chemical Industry. *Chemical Industry & Chemical Engineering Quarterly , 15* (1), 5-8.

- easy to understand and policy-relevant,
- normative (possibility to compare to a baseline situation),
- scientifically sound and statistically valid,
- responsive to change in time and space,
- technically feasible and cost-efficient in terms of data collection,
- useable for scenarios for future projections,
- allowing the comparison between the organizations, communities and states and
- user-driven.

Choudry et al create three groupings of safety performance indicators[85] (as described for the construction industry) as markers for the establishment of a safety culture (and, by extension, possibly to a well-functioning biorisk management system). They group indicators into safety climate, behavior-based indicators, and metrics from management. Jovasevic-Stojanovic and Stonjanovic use a slightly different perspective to categorize indicators for safety management systems into three main groupings,[86] which can be applied to biorisk management systems. Management performance indicators provide information about management efforts to improve the organization's biosafety and biosecurity performance. Operational performance indicators give information about the biosafety and biosecurity performance of the organization's technical operations. Biorisk status indicators are the information about accidents, incidents, and near-misses, as well as their consequences.

Biorisk climate indicators

Biorisk climate indicators emphasizes perceptions held by employees regarding the importance of managing biorisks in their organizations by measuring employee perceptions of management commitment to the issues, detecting areas of biosafety and biosecurity that require improvement, identifying trends in an organization's biorisk management performance, and establishing benchmarks for various levels of biorisks of different organizations. There is a plethora of literature on safety climate, including many different tools, analyses, and results. All indicate the value of measuring this perceptional contribution to safety performance. Most of the authors agree that safety climate has an impact on processes such as communication, decision-making, problem-solving, conflict resolution, attitudes, and motivation, whether these can be measured directly or indirectly.[87] Many papers give exemplar safety climate questionnaires[88] that may be useful starting

[85] Choudry, R. M., Fang, D., & Mohamed, S. (2007). Developing a Model of Construction Safety Culture. *Journal of Management in Engineering , 23* (4), 207-212.
[86] Jovasevic-Stojanovic, M., & Stonjanovic, B. (2009). Performance Indicators for Monitoring Safety Management Systems in Chemical Industry. *Chemical Industry & Chemical Engineering Quarterly , 15* (1), 5-8.
[87] Diaz, R. I., & Cabrera, D. D. (1997). Safety climate and attitude as evaluation measures of organizational safety. *Accident Analysis and Prevention , 29* (5), 643-650.
[88] DeJoy, D. M., Gershon, R. R., & Schaffer, B. S. (2004, July). Safety Climate: Assessing management and organizational influences on safety. *Professional Safety* , 50-57; Gershon, R. R., Karkashian, C. D., Grosch, J., Murphy, L. R., Escamilla-Cejudo, A., Flanagan, P. A., et al. (2000).

points for modification to determine "biorisk" climate. For example, Gershon et al have a safety climate questionnaire[89] that is widely cited and the table below gives some examples of how items could be adapted to biorisk.

Sample Safety Climate Questionnaire Items	**Example Adaptation for a Possible Biorisk Questionnaire Item**
Safety Program Elements: "On my unit, written safety policies are always available."	Biorisk Program Elements: In my laboratory, written biorisk policies are always available.
Support for Safety Programs: "Where I work, employees are encouraged to make suggestions for improving work safety."	Support for Biorisk Programs: Where I work, employees are encouraged to make suggestions for improving biosafety and biosecurity.
Senior Management Support for Safety: "On my unit, senior level management gets personally involved in safety activities."	Senior Management Support for Biorisk: In my laboratory, senior level management gets personally involved in biorisk activities.
Communication and Feedback about Safety: "On my unit, communication is open between supervisors and staff."	Communication and Feedback about Biorisk: In my lab, communication is open between supervisors and staff.
Accountability and Responsibility: "On my unit, my compliance with Universal Precaution procedures and practices is part of my annual written evaluation."	Accountability and Responsibility: In my lab, my compliance with biosafety and biosecurity policies and procedures is part of my annual written evaluation.
Accessibility, Availability, and Quantity of Safety Equipment and Supplies and Engineering Controls: "On my unit, personal protective equipment is readily available and accessible."	Accessibility, Availability, and Quantity of Biorisk Equipment and Supplies and Engineering Controls: In my lab, needed biorisk tools (e.g. PPE, inventory software) are readily available and accessible.
Design, Maintenance, and Housekeeping of the Work Site: "My work area is not cluttered."	Design, Maintenance, and Housekeeping of the Work Site: My work area is not cluttered.
Training and Education: "My hospital offers training classes or special seminars on bloodborne pathogens."	Training and Education: My institution offers training classes or special seminars on biorisk issues.
Absence of Job Hindrances to Safety: "I have enough time at work to always follow Universal Precautions."	Absence of Job Hindrances to Biorisk: I have enough time at work to always follow good biosafety and biosecurity procedures.

Behavior-based biorisk indicators

This is essentially a somewhat simple mechanism where randomly sampled observations of worker's behavior are evaluated as to whether the observed behavior is "safe and secure" or "not safe or secure." Glendon et al suggest[90] that behavior observation data are superior to accident statistics as they focus on unsafe behavior prior to accidents occurring and are sensitive to changes, allowing for more immediate identification of some types of problems. The ratio of desired behavior can be calculated simply by dividing the total observed desired behavior

---

Hospital safety climate and its relationship with safety work practices and workplace exposure incidents. *American Journal of Infection Control , 28* (3), 211-221; Turnberg, W., & Daniell, W. (2008). Evaluation of a healthcare safety climate measurement tool. *Journal of Safety Research , 39*, 563-568.

[89] Gershon, R. R., Karkashian, C. D., Grosch, J., Murphy, L. R., Escamilla-Cejudo, A., Flanagan, P. A., et al. (2000). Hospital safety climate and its relationship with safety work practices and workplace exposure incidents. *American Journal of Infection Control , 28* (3), 211-221.

[90] Glendon, A., & Litherland, D. (2001). Safety climate factors, groups differences and safety behaviour in road construction. *39*, 157-188.

by the total observed desired and undesired behavior. To utilize behavior-based biorisk observations, necessary resources include a simple and consistent checklist where behaviors can be identified as desired or undesired,[91] trained observers (training all or most workers in the observation process facilitates long-term acceptance of these observational indicators), and a process that is supported by both workers and management. Geller et al. provide ten guidelines for implementing a behavior-based coaching process:[92]

1. Teach procedures (training) with principles (education) – refers to both safety training and training observers
2. Empower employees to own the process – "critical behavior checklist" is developed via interactive group discussion by line workers and supported by management
3. Provide opportunities for choice – management should provide structure, instruction, and support for safety, while providing opportunities for employees to develop procedural options and choose among these, wherever possible.
4. Facilitate supportive involvement from management – organizational leaders must walk the fine line between supporting the process and driving the process
5. Ensure that the process is non-punitive
6. Ensure that the observer is nondirective – observer is not responsible for corrective action but merely completes critical behavior checklist and shows observee the results.
7. Progress from announced to unannounced observations
8. Focus on interactions, not just numbers – metric is just part of the system
9. Continuously evaluate and refine the process
10. Make the process part of a larger effort – it must be viewed as one of many systematic ways to provide a safe and secure workplace

An excellent side-benefit of behavior based approaches is that a safety and security observation process can function to increase desired behaviors of the observers. In other words, if employees conduct observations of peer performance, their own performance may improve.[93] Furthermore, behavior-based approaches can spur "supervisory-based intervention program"[94] where supervisory priorities are aligned with strategic priorities (e.g. biorisk policies) and front-line supervisors are encouraged to express high safety and security priorities during daily exchanges with workers. A criticism of the implementation of some behavior-based observations is that they overemphasize behavior controls at the expense of

[91] Cooper, M., & Phillips, R. (2004). Exploratory analysis of the safety climate and safety behavior relationship. *Journal of Safety Research , 35*, 497-512.
[92] Geller, E. S., Perdue, S. R., & French, A. (2004, July). Behavior-based Safety Coaching. Professional Safety , 42-49.
[93] Alvero, A. M., Rost, K., & Austin, J. (2008). The safety observer effect: The effects of conducting safety observations. *Journal of Safety Research , 39*, 365-373.
[94] Luria, G., & Rafaeli, A. (2008). Testing safety commitment in organization through interpretations of safety artifacts. *Journal of Safety Research , 39*, 519-528.

improving unsafe and unsecure conditions, which can lead to a "blame the worker" mindset.[95] Behavior observation approaches can sometimes be merged with overall efforts to change the safety and security culture in the workplace. [96]

Biorisk performance indicators

The newly released Organisation for Economic Cooperation and Development (OECD) *Guidance on Developing Safety Performance Indicators related to Chemical Accident Prevention, Preparedness and Response*[97] is a very valuable tool in developing performance indicators for a biorisk management system. The OECD document suggests the following categories for establishing safety performance indicators (astericks indicate categories that are unlikely to be found in laboratory biorisk settings); most of these concepts readily extend to biorisk management systems as shown by the notes in brackets:

a. Policies, Personnel and General Management of Safety
    i. Overall Policies
    ii. Safety [Biorisk] Goals and Objectives
    iii. Safety [Biorisk] Leadership
    iv. Safety [Biorisk] Management
    v. Personnel
    vi. Internal Communication/Information
    vii. Working Environment
    viii. Safety [Biorisk] Performance Review and Evaluation
b. General Procedures
    i. Hazard Identification and Risk Assessment
    ii. Documentation
    iii. Procedures
    iv. Management of Change
    v. Contractor Safety [Addressing safety and security of contractors onsite for maintenance, etc through escorting and other procedures]
    vi. Product Stewardship[could be generalized to material control and accountability]
c. Technical Issues
    i. [Research and Development – note: these SPIs would apply in the procedures section above since that is the core mission of most labs]
    ii. Design and Installation
    iii. Inherently Safer [and More Secure] Processes
    iv. Industry Standards
    v. Storage of Hazardous Substances (HazComm)

---

[95] Wirth, O., & Sigurdsson, S. O. (2008). When workplace safety depends on behavior change: Topics for behavioral safety research. *Journal of Safety Research , 39*, 589-598.

[96] DeJoy, D. M. (2005). Behavior change versus culture change: Divergent approaches to managing workplace safety. *Safety Science , 43*, 105-129.

[97] OECD Environment Directorate. (2008). *Guidance on Developing Safety Performance Standards related to Chemical Accident Prevention, Preparedness and Response* (Vol. No. 19). Paris, France: OECD Environment, Health, and Safety Publications.

vi. Maintaining Integrity/Maintenance

d. External Cooperation
   i. Cooperation with Public Authorities
   ii. Cooperation with the Public and Other Stakeholders
   iii. Cooperation with Other Enterprises
e. Emergency Preparedness and Response
   i. Internal (on-site) preparedness planning
   ii. [External (off-site) preparedness planning]
   iii. [Cooperation Among Industrial Enterprises]
f. Accident/Near-Miss Reporting and Investigation
   i. Reporting of accidents, near-misses and other "learning experiences"
   ii. Investigation
   iii. Follow-up, including application of lessons learned and sharing of information

Returning to Jovasevic-Stojanovic and Stonjanovic's structure of performance indicators,[98] we can easily see how these examples in the table below map with the OECD categories and the potential usefulness for looking at the effectiveness of biorisk management systems.

Management Performance Indicators	Number of accident and near-misses reports; number of program inspections; number of meetings, trainings, and audits on biorisk topics; trends in public information, awareness, and trust
Operational Performance Indicators	Number of component malfunctions and damages; maintenance hours per operation hour; number of non-authorized access to the facility
Biorisk Status Indicators	Number of laboratory-acquired infections; economic losses; number of releases from containment

Incident reports

Incident reports are just one small part of measuring performance of a biorisk system. Using objective accident data to measure safety performance is notoriously problematic because such data are insensitive, of dubious accuracy, retrospective, ignore risk exposure, and tend to be very unstable.[99] Near misses are difficult to collect. There is a huge set of literature on error detection, but this is in

[98] Jovasevic-Stojanovic, M., & Stonjanovic, B. (2009). Performance Indicators for Monitoring Safety Management Systems in Chemical Industry. *Chemical Industry & Chemical Engineering Quarterly , 15* (1), 5-8.

[99] Fernandez-Muniz, B., Montes-Peon, J. M., & Vazquez-Ordas, C. J. (2007). Safety Culture: Analysis of the causal relationships between its key dimensions. *Journal of Safety Research , 38*, 627-641.

mechanically based systems like aviation control and processing plants with automation; in a biorisk setting, this type of information could theoretically be collected on some of the engineered controls through the building management system and access control system. Staff are often reticent about reporting accidents. The concept of an "accident-free" period can suppress accident reporting. Implementation of a safety management system implies an improvement in the recording of accidents/incidents so more are recorded. So, while performance may improve, the indicator (accidents) actually indicates a worsening. When rewards or incentives are tied to improvements in injury rates rather than safety-related behaviors and near misses, a disincentive for injuring reporting may occur.[100]

Reporting is obviously a challenge that begins with first defining what is reportable. The CWA 15793 defines incident as "event with potential for causing harm;" this definition is broad enough to encompass both accidental (biosafety) and intentional (biosecurity) events. Once an acceptable definition that is understood by the appropriate stakeholders is in place, then the disincentives in the previous paragraph must be overcome if a meaningful reporting system is going to be established. Recognizing the need for improved biorisk incident reporting, the *Select Agent Program and Biosafety Improvement Act of 2009*[101] (pending in Congress at the time this report was drafted) would require the establishment of a "Biological Laboratory Incident Reporting System." Biorisk incidents reported either internally or those that become public knowledge (see Appendix A) are not converted into an incident rate or otherwise typically put into context. If incidents are reported at all, they are not converted into a rate, due to lack of tracking or consideration of an appropriate denominator (e.g. number of hours worked, number of people working with a given category of pathogens, amount of containment laboratory space, etc). This lack of a denominator makes it impossible to know if the biorisk incident rate is improving or worsening over time. In contrast, the following text box gives some examples of how incident rates are calculated by some government agencies and industries.

[100] Wirth, O., & Sigurdsson, S. O. (2008). When workplace safety depends on behavior change: Topics for behavioral safety research. *Journal of Safety Research , 39*, 589-598.
[101] H.R. 1225; http://www.opencongress.org/bill/111-h1225/show

OSHA Incidence Rate Formula

$$\text{Incident rate} = \frac{\text{Number of cases x 200,000}}{\text{Actual hours worked}}$$

Where 200,000 is the hours worked by 100 full time employees per year (monthly would be 16,666.67, quarterly 50,000). The Incidence Rate formula should take into account changes in the number of employees or the hours of exposure (hours worked), so the rate of injury can be the same even if more or less employees are working more or less hours. A calculator is available on the Bureau of Labor Statistics website (http://data.bls.gov/IIRC/).

National Institute for Occupation Health & Safety (NIOSH) Formula

$$\text{Incident rate} = \frac{\text{Number of cases}}{\text{100 Full time workers}}$$

NIOSH's Work-RISQS is a web-based public access query system for obtaining national rates for nonfatal occupational injuries and illnesses (http://www2a.cdc.gov/risqs/wrinjrate_ns.asp).

The Patient Safety Handbook

$$\text{Incident rate} = \frac{\text{Number of incidents}}{\text{(population at risk)*(time population at risk)}}$$

Employed by hospitals for monitoring incidents, the handbook says that for incident reporting the denominator includes the population at risk for the event of interest multiplied by the time that the population was at risk. The incidence rate is the number of new cases per unit of person-time at risk. Using person-time rather than just time handles situations where the amount of observation time differs between people, or when the population at risk varies with time. Hospitals also use a measurement known as *patient-days* for the denominator in certain calculations. Patient-days try to reflect the volume of patients per day (or census period) in an area of a hospital.

Federal Aviation Administration

$$\text{Incident rate} = \frac{\text{Number of accidents}}{\text{100,000 hours flown}} \quad \text{OR} \quad = \frac{\text{Number of accidents}}{\text{Active pilots}}$$

These are used by the FAA for general aviation accident rates.

There are a series of steps for institutions to consider if they want to implement an effective incident notification and response protocol (NRP).[102] Some incidents that should be reported and investigated do not carry concern for harm; a risk assessment will discern whether the incident is also a serious incident or a near-miss, or remains merely a reportable occurrence as part of a performance indicator system. Thus, to start with, a NRP can have risk-based tiers and the expected report should contain six key questions:[103] who (involved person(s), witnesses, supervisor(s), investigators, and medical), what (description of incident, any harm caused – exposure, release, theft, sabotage, or loss), when (date, time, point in procedure of incident), where (location, facilities, equipment used, under what conditions), why (what actually caused the incident – see following discussion on root cause analysis), and how (how can a recurrence of the incident be prevented). Once the NRP is developed, communication and training are needed so that all involved understand their roles and responsibilities.

In the event of an incident, the NRP is activated. First, the risk level is determined; a flow chart is a simple tool that can be designed for this step.[104] An investigation is conducted to collect basic information and then a root cause analysis (see following text boxes) should be done to help figure out what caused the incident. The results of this investigation and analysis need to be communicated and a corrective/preventative action plan should be developed. This corrective action plan should recommend actions that would make it very difficult, if not impossible, for the incident to recur. Corrective action is a short-term solution to directly address the item of non-conformance while preventative action is a long-term, more systemic approach to addressing underlying issues. [105] For example, if training is lacking a corrective action may be to immediately replace the person requiring training with a fully-trained person and to schedule and provide training for the un-trained staff member. In this example, preventive action may be the institution or revision of a training plan for persons previously unidentified or implementation of more stringent demonstrations or competency after training. A process must be in place to assure: roles and responsibilities are identified for each corrective and preventative action; when and how to take action is determined; if technical and/or managerial actions require consideration or revision; and timely implementation of recommendations/establishment of deadlines. Analysis of aggregated incidents is warranted to determine common or systemic problems/trends

To implement effective and appropriate corrective and preventative actions, it is important to understand what led to the incident through a formal root cause

[102] Coghlan, K. (2008, January). Investigating Laboratory Accidents. *Safety Professional* , 56-57.
[103] http://www.osha.gov/SLTC/etools/safetyhealth/mod4_factsheets_accinvest.html
[104] personal communication, Burnett, Coberley, & Denison, August 2009.
[105] Burnett, L. C. (2006). Biological Safety Program Management. In D. O. Fleming, & D. L. Hunt (Eds.), *Biological Safety: Principles and Practices* (pp. 405-415). Washington, D.C., USA: ASM Press.

analysis. There are many models for these analyses,[106] ranging from very complex to quite simple. Two simple models that are likely useful for conducting root cause analyses on a wide range of biorisk incidents include "The five whys"[107] (see textbox for example) and the KATTAR model.[108] The KATTAR model evaluates an incident on the following factors: Knowledge (did the worker know the principles behind why s/he should be following a certain procedure?), Assignment (was the worker supposed/ready to be assigned to the procedure?), Training (did the worker have the training to conduct the specific procedure?), Tools (were the appropriate tools available to conduct the procedure safely and securely?), Accountability (did management take responsibility for providing workers and supervisors with the appropriate knowledge and training; assigning them to appropriate procedures; and provide them with appropriate tools?), and Resources (were appropriate resources provided for the procedure to be performed safely and securely?).

Applying "the five whys" to an example of a needlestick with an infectious agent:

Q1; Why did the worker get stuck with a needle?
Al: Because the researcher was not careful or familiar with using this device.

Q2: Why was this the case?
A2: The researcher normally used a single channel pipette to transfer the potentially pathogenic material. This time, however, that type of pipette was not available.

Q3: Why was that type of pipette not available?
A3: Because it was broken and the laboratory manager did not order any more.

Q4: Why did the lab manager not order more?
A4: Because he did not know there were no more working pipettes.

Q5: Why did the laboratory manager not know there were no more working pipettes?
A5: Because the laboratory does not have a system to track equipment.

[106] Lundberg, J., Rollenhagen, C., & Hollnagel, E. (2009). What-You-Look-For-Is-What-You-Find - The consequences of underlying accident models in eight accident investigation manuals. *Safety Science , in press.*
[107] Coghlan, K. (2008, January). Investigating Laboratory Accidents. *Safety Professional* , 56-57.
[108] Roig, R.A. 2004. *ISO 14001 - Environmental Management Systems: A Complete Implementation Guide*. Specialty Technical Consultants, Inc. North Vancouver, British Columbia, Canada.

Risk Communication is Key to Effective Risk Governance

The risk governance framework given in the IRGC guidance document identifies four top-level functional areas:

- Pre-Assessment
- Risk Appraisal
- Tolerability and Acceptance Judgment
- Risk Management

Between all these components, the IRGC have identified a key capability: communication. Although communication in their document is probably meant to represent face-to-face, telephone, traditional print media (magazines, newspapers, flyers), and traditional broadcasting (radio and TV), this section focuses on Internet-based social software media channels to satisfy the needs for outward communication as well as for collaboration among teams. As the bioscience enterprise becomes more diverse and global, it is imperative to continually reach out to stakeholders in formats that are familiar to them. Social networking is the most rapidly growing communication forum:[109] 96% of Generation Y has joined a social network, Facebook reached 100 million users in nine months (if it was its own country, it would be the 4th largest), and studies have shown Wikipedia to be more accurate than traditional encyclopedias like Encyclopedia Britannica.

Social media is a benign term for the over-loaded phrase "Web 2.0." As it is used today, social media includes a wide variety of systems that provide a means for two-way interaction via the Internet. These systems differ from standard webpages in that user input is solicited and even required in some cases. Such systems gain in utility as the number of users, especially active contributors, increases.

Categories of social software (examples in parentheses) include:

- Microblogging (Twitter, Identica)
- Blogging (Blogspot, WordPress.com)
- Wikis (Wikipedia, Intellipedia)
- Forums, online discussions, and e-mail list services (Yahoo! Groups, Google Groups)
- Document collaboration systems (SharePoint, Google Docs, Scribd)
- Tagging (Evidenced by Delicioius, Flickr, WordPress)
- Social bookmarking (Delicious, Digg)
- Online rating systems (Amazon, Digg)
- Content management systems (Plone, Drupal)
- Social networking (Facebook, LinkedIn, Twitter)
- Photo sharing (Flickr)
- Podcasting and video-sharing (YouTube)
- Online distributed office applications (GoogleDocs)

[109]Socianomics, posted to YouTube July 30, 2009.http://www.youtube.com/watch?v=sIFYPQjYhv8

This list is not only incomplete, but also almost assuredly obsolete the moment it was assembled. New social software systems are being created daily.

Software tools under consideration in this report must perform a number of functions. Foremost among them are tools that facilitate the exchange of information among risk professionals. At the same time these systems must communicate risk appropriately to the general public. The wide dissemination of best available knowledge with suitable controls to protect draft and otherwise sensitive material is the overall goal.

To that end social software systems are sought that permit a balanced presentation of factual knowledge along with personal interests, concerns, beliefs, and resources. This will need to allow the exchange of risk perceptions as well as conceptual aspects of the problem under consideration. These tools decision makers will need to elicit concerns while helping stakeholders and the public understand the rationale and decision results. These systems will also be useful for fostering tolerance for conflicting viewpoints and forming the basis for resolution. Additionally, they will create trust in the institutional processes by building peer relationships and friend of a friend (FOAF) networks that aid in vetting the expertise, authenticity, and credentials of collaborators.

Besides addressing the requirement for helping risk professionals and civil society make informed choices, social software should organize the feedback from the public. As such, these systems will have an impact on how society copes with risk.

Applicability of tools to risk governance

	Micro-blogging	Blogging	Wikis	On-line discussions	Document Management	Social bookmarking	Online rating	Content Management	Social networking	Podcasting	Distributed Applications
Pre-Assessment											
Problem Framing		X		X	X		X			X	X
Early Warning	X	X						X	X		
Screening			X						X		
Determination of Scientific Conventions	X		X		X			X	X		

	Micro-blogging	Blogging	Wikis	On-line discussions	Document Management	Social bookmarking	Online rating	Content Management	Social networking	Podcasting	Distributed Applications
Risk Appraisal											
Risk Assessment											
Hazard Identification & Estimation	X	X	X	X							
Exposure & Vulnerability Assessment					X		X				X
Risk Estimation			X	X	X			X			X
Concern Assessment											
Risk Perceptions	X	X		X			X	X			
Social Concerns	X	X		X			X	X	X	X	
Socio-Economic Impacts			X		X	X	X				X
Tolerability & Acceptability Judgment											
Risk Evaluation											
Judging the Tolerability & Acceptability		X		X	X		X	X	X		X
Need for Risk Reduction Measures	X	X	X	X	X	X		X	X		X
Risk Characterization											
Risk Profile				X	X			X			X
Judgment of the Seriousness of Risk		X		X			X		X		
Conclusions & Risk Reduction Options					X			X	X		X

	Micro-blogging	Blogging	Wikis	On-line discussions	Document Management	Social bookmarking	Online rating	Content Management	Social networking	Podcasting	Distributed Applications
Risk Management											
Implementation											
Option Realization					X			X			X
Monitoring & Control	X	X		X						X	X
Feedback from Risk Mgmt. Practice	X	X		X				X	X	X	
Decision Making											
Option Identification & Generation			X	X	X	X					X
Option Assessment				X			X	X		X	
Option Evaluation & Selection	X	X		X			X	X			

Pre-Assessment

Tools that assist with dynamic, shared creation of documents related to framing of the problem will have a positive impact on this phase of the risk management framework. These would be blogging, online discussions, document management systems, and distributed applications such as Google Docs. Additionally, online rating systems would allow strength of opinion to be monitored. Video podcasting might allow professionals to better illustrate aspects of the problem domain. These tools can facilitate sharing between stakeholders, helping to better identify risks.

Early warning establishes whether there are signals of the risk that would indicate its realization. This step also investigates the institutional means in place for monitoring the environment for such early warning signals. Microblogging and blogging could find use as statement of health indicators from the public at large and could be early indicators of any release from a bioscience facility. Specialized content management systems could be part of an instrumented system of measurement for determining early warning.

Conducting preliminary probes into hazards and assigning a risk to pre-defined assessment and management 'routes' might be aided by wikis for online assembling of expert knowledge and social networks for maintaining connections between

experts in separate fields. The Biosafety Risk Assessment wiki[110] is a prime example of the applicability of this type of forum to biosafety risk identification and understanding.

The selection of major assumptions, conventions and procedural rules for assessing the risk as well as the emotions associated with it could be facilitated with professional wikis, document management collections, some level of social networking, and possibly a content management system customized to display the aggregated information.

Risk Appraisal

All manner of collaborative information gathering, microblogging, blogging, wikis, and online discussions would be useful in collecting hazard information. An online rating system could be included to help with estimating probabilities and obtaining subjective views on hazard likelihood and consequences of different scenarios of concern.

Because vulnerability assessment lies within a more objective area, experts could benefit from online discussion areas, wikis, document management systems, or distributed applications to avoid a glut of draft documents attached to e-mails.

Determining the probability of occurrence of an event is a difficult task for professionals. Transparently communicating the results of a process that involves categories of "complexity," "uncertainty," and "ambiguity" will be fraught with opportunities for misunderstanding. The use of wikis, discussion forums, document management tools, and/or distributed applications will help produce these probability estimates. Content management systems could help with communicating the results to both stakeholders and the public.

Acquiring information about stakeholders' concerns, questions, and apprehensions is a particularly ripe area for social software application. Microblogging, blogging, online discussions, online rating systems, and content management mechanisms could be useful tools for capturing subjective information about hazards.

Social consequences could easily make use of all the above as well as shared taxonomies (social bookmarking), social networking to connect different external groups, and podcasting to capture graphical depictions of concerns.

Socio-economic impacts require interdisciplinary analysis and expertise. Wikis, document management systems, social bookmarking, online rating systems, and possibly distributed models as online applications could be highly effective.

Tolerability & Acceptability Judgment

Judging acceptability or tolerance of a risk and determining the need for risk reduction requires broader value-based assessments. Such issues, which include

[110] www.biosafetyriskassessment.org

the choice of technology, societal needs requiring a given risk agent to be present, and the potential for substitution as well as for compensation, reach beyond the risk itself and into the realm of policy-making and societal balancing of risks and benefits. Virtually all social software tools could come into play.

Risk characterization compiles scientific evidence based on the results from the risk appraisal phase. Blogging, online discussions (but with restricted audiences), document management, online ratings, content management, some level of social networking, and perhaps specialized online applications could be effective in this phase.

Risk Management

The six steps of the risk management phase are fertile ground for social software applications. All aspects under consideration here find at least some level of utility. Monitoring, control, and feedback portions of the process can make good use of most social software tools.

CONSIDERATIONS FOR SUSTAINABLE RISK GOVERNANCE AT BIOSCIENCE FACILITIES

Laboratory biorisk management is increasingly seen as a major aspect of the development and sustainability of activities with biological hazards. This is true in economically developed countries, where a broad spectrum of biomedical and biotechnological activities is already in place and in many cases still increasing, and in developing countries where a real effort is made to develop biological activities to respond their biomedical, agricultural, industrial or commercial needs. While the importance of developing activities in the field of biology has been widely recognized, the importance of managing biorisk efficiently to ensure their sustainability and prevent biological threats worldwide has also been pointed out by numbers of experts from governmental and non-governmental organizations.

In a limited inquiry made in the framework of this project towards various governmental, academic and private organizations from different countries around the world (see Appendix E), about 25% of the responders mentioned examples of biocontainment facilities that could not be used at all or could not be used at the planned level of containment or performance. This was mostly but not exclusively the case for institutions from developing countries. Reasons invoked included lack of compliance, lack of technical and financial means, and lack of knowledge and skills. The same proportion of responders mentioned significant delays (more than 6 months) only due to lack of compliance or resistance of the community or authorities, without considering delays due to technical problems and poor project management. The authors of this report also know of multiple examples of costly up-grades of biocontainment facilities required shortly after completion of their construction, due to either a poor initial risk evaluation or a change in the project orientation.

A wider international expert survey on emerging biorisks related to occupational safety and health[111] pointed out poor risk assessment as the main emerging biorisk issue besides the emergence of new and drug-resistant organisms, before the lack of information and training on biorisk and poor maintenance of water and air systems. In general, knowledge and skills, together with the availability and effectiveness of operational means, appear as the major issues for the sustainability of biorisk management.

Based on these observations, this section of the report aims to articulate the processes, knowledge and skills that are required to avoid such problems and ensure the sustainability of biological activities, both in planning for and building biocontainment facilities and in managing biorisk during operations.

Preliminary considerations

Sustainability, relevance, effectiveness, and efficiency

The sustainability of a process or system is tightly bound to its relevance, effectiveness and efficiency. If not relevant, effective and relatively efficient, a process or a system has no chance to reveal sustainable in the distance. Conversely, a process or a system that, for any reason (lack of financing, logistic issues, changes in external factors…), does not appear sustainable over time, will not remain relevant, effective and efficient. From this standpoint, sustainability should be considered an intrinsic value of any process or system evaluation or decision making, not a separate evaluation criterion. This certainly applies to biorisk management and to the design and construction of biocontainment facilities.

Well-designed and constructed facilities are considered an important and effective support to good operational and management practices. However, biocontainment facilities generally require significant investment and generate high operational costs. As they can be seen as the "hardware" that is not only expensive but also much less adaptable than operational and management practices, their design and construction, as well as the decision to build such facilities, should be challenged and submitted to a sound evaluation of their relevance, effectiveness and efficiency in order to assess and ensure their sustainability.

Sustainability, risk governance, and biorisk management

The laboratory biorisk management standard is to be used in organizations that are in operation, in order to manage the biological risk of their current and future activities. It is not meant and cannot be used to help in the decision making that takes place prior to the operational phase, such as the decision to launch new research programs, to develop activities at a larger scale or to invest in new biocontainment facilities or facilities of a higher containment level, for instance. This kind of decision is still crucial for the organization, because it will influence its future and could have a major impact in terms of risk control and operational

[111]Expert forecast on emerging biological risks related to safety and health, European Risk Observatory Report, 2007 (http://osha.europa.eu//en/publications/reports/7606488/).

costs. Unsound decisions at that stage can result in situations that may ultimately be unsustainable and pose major concerns with respect to biosafety and biosecurity over the lifetime of the facility. Examples of this are the facilities that have been built but cannot be used under normal, safe operating conditions because operating constraints and costs were underestimated during the initial decision phase. Adopting the concepts of risk governance in biorisk management to both operational facilities and for facilities in the planning stages should allow sound decision making before and during operations and ensure effective and sustainable risk management provided the appropriate knowledge and skills are available at each stage of the process.

Prior to operations – planning for sustainability during construction

Preliminary risk assessment and decision making

Any project, be it to launch a new scientific program, expand biological activities to a larger scale or build a biocontainment facility, starts with decisions at a strategic level. These are taken by senior management, most of the time on the basis of a preliminary exploration and a number of economical, scientific or sociological considerations. When construction is concerned, these considerations and their supporting data are classically collected and presented in a preliminary study, or feasibility study, that is based on the user's requirements and includes a first budget and time line appraisal. In general, the final decision is taken on these bases by a limited number of people, with a variable consulting input.

The small inquiry made in the framework of the current project (Appendix E) has shown that the main decisions regarding the construction of biocontainment facilities are indeed taken by senior management, in general with some input from the biosafety professional, the facility manager and the technical staff. Long-term considerations such as resource availability or other continuity issues are taken into account in about 75% of the cases, but there is generally no well-established process to define and analyse the needs, constraints and risks prior to deciding.

The purpose of the decision making at this stage is (1) to decide to launch the project or not, and (2) to identify the required resources, processes and tools to put in place in order to manage the project-related risks in an appropriate way. This requires a global view that integrates all the significant aspects of the project in a balanced, comprehensive perspective. This becomes particularly challenging when building facilities that are designed with an intentional flexibility to meet not just current needs but also for future capabilities and surge capacity. In these cases, the preliminary risk assessment and decision-making phase needs to state specifically what the facility will not be able to accommodate from a biorisk perspective.

While senior management are usually familiar with strategic thinking and with economic, financial and scientific and/or commercial issues, they might be less prone, without aid, to apprehend the possible impact of all or at least some of the technical, regulatory or logistic aspects that may, in a complex matter as the construction and running of biocontainment facilities, threaten the project viability.

Even when looking for ad hoc advice, top management may be limited by the lack of availability of appropriate competencies. They might also underscore the importance of perception in the general, non scientific community. There are cases where unexpected reactions from the community and the authorities have seriously delayed the development or normal use of a biocontainment facility, and many others where non expected logistic constraints and running costs have limited or prevented their use according to planning.

As a reaction to such failures, more and more financing agencies run or require from the demanding institution a documented preliminary risk assessment of the project prior to any financing decision regarding the construction of biocontainment facilities. The extent to which the various possible issues are taken into account and analysed still varies quite significantly from one institution to another.

Carrying out a preliminary but comprehensive risk assessment before the decision to start any biocontainment construction project would contribute to prevent major failures during or after the design and construction process and ensure the sustainability of the facilities and associated activities. The purpose of this preliminary project risk assessment is to capture and evaluate the issues that may impact significantly the development and sustainability of the project during the construction phase and when the facilities will be in operation. This should be done while defining the project justification, objectives and general concepts. Results of the preliminary project risk assessment should be documented together with the project description in the feasibility study. These results should be available to senior management, financing bodies and other major stakeholders.

Such a preliminary project risk assessment appears perfectly in line with the risk governance precepts[112]. As discussed earlier, the pre-assessment should include problem framing, early warning and monitoring, early screening, and looking at processes and tools to further assess risks and risk perceptions. Within the context of planning for a project, problem framing should help the project stakeholders develop a common understanding of the project-related issues and identify possible differences in risk perception. Early warning and monitoring activities can help the project team identify all possible indicators of risks and threats to the project, including external ones (e.g. regulations and regulatory changes, socio-economic factors, political situation, and public perception of biorisk or the projected activities).

For small, routine or relatively simple projects in favourable settings, such a pre-assessment may appear sufficient to decide to launch a construction project on sound bases. In other situations it may not be sufficient to obtain a satisfying level of guarantee or it may reveal risks that appear likely to jeopardize the project or its long term sustainability. Such cases would require more complete appraisal before deciding to start the project. This appraisal should comprise a technical risk assessment as well as a concern assessment to evaluate risk perceptions and socio-

[112]"White paper on Risk Governance", The International Risk Governance Council, 2006 (http://www.irgc.org/The-IRGC-risk-governance-framework,82.html).

economic concerns more completely. The overall purpose of this comprehensive risk appraisal is to identify the risk treatment options more precisely and to lead to an informed judgement on the tolerability and acceptability of the residual risk.

With respect to sustainability, preliminary project risk assessment should deal with at least the following aspects:

- suitability and adequacy of the project objectives to respond economic needs in the expected future socio-economic environment;
- scientific and technical feasibility of the planned scientific program;
- adequacy of the project conception to the project needs and objectives;
- availability and continuity of appropriate project financing capacity;
- risk acceptability of the projected activities (reality of the biorisk and perception in the concerned community);
- environmental, socio-economic and cultural acceptability of the project and projected activities (environmental impact and perception, socio-economic impact in the area, cultural perception…);
- availability of qualified resources for the project design, management and execution;
- availability of human, logistic and financial resources to run and maintain the facility;
- long-term commercial viability of the activities (or availability of subsidies in case of non-commercial projects)…

When compared to the way feasibility studies are usually performed, such an approach would definitely be more focussed on risk assessment, take a wider range of factors into account, and consider the sustainability of the entire project in a more complete manner, including after construction is completed.

Since the aspects that are considered affect various disciplines, different possibly specific tools are likely to be used to reach the risk assessment objectives. General, widely used analytic tools like the SWOT (Strengths - Weaknesses - Opportunities - Threats) analysis can be used to help tackling specific issues or summarize and communicate the overall results of the preliminary project risk assessment.

The aspects taken into consideration in the preliminary project risk assessment cover a large variety of issues that comprise but are much wider than biorisk management. They are still of a capital importance for the sustainability of any project involving the construction and future use of a biocontainment facility, and therefore for a sustainable biorisk management.

The usual skills of senior management (e.g high level managerial, economical, financial and/or scientific backgrounds and experience, "helicopter view", strategic sense, and a decision-oriented mind) are required to sponsor the preliminary project risk assessment and take appropriate decisions.

Depending on their own experience, a number of economic, financial, scientific or general issues can be dealt with by senior management directly, without much external aid. However, given the multiplicity and specificity of some of the aspects

that need to be considered, they are likely to benefit from an access to additional, more specific knowledge and skills, such as:

- legal and regulatory expertise regarding health and safety, biosafety, biosecurity, as well as environment and permitting;
- expertise in biosafety and biosecurity, experience in biorisk management;
- in-depth scientific knowledge and expertise of the biological agents and processes;
- experience in managing or participating to similar construction projects;
- operational experience of managing and maintaining similar biocontainment facilities;
- experience in managing or participating to construction projects in the same region, or a comparable region;
- experience in logistic supply (natural resources, utilities, equipment from abroad…);
- ad hoc expertise in animal facilities, greenhouses, large-scale production…;
- expertise in compliance, human resources, business continuity…;
- access and communication with local stakeholders…

Access to such a wide range of knowledge and skills is possible through consulting, either internally if resources are available, or externally (access to nationally or internationally active consultants). Given the importance of the preliminary risk assessment for the conception and sustainability of the entire project, appropriate external consulting at that stage may be extremely cost-effective. The realisation of the risk assessment report and feasibility study gathering all the project essentials can also be out contracted. However, while the risk assessment and feasibility study can be carried out efficiently by external consultants, in-house ownership of the risk management and its outcome appears essential.

Biocontainment design and construction

Design and construction projects are traditionally managed according to a well-established process that may vary slightly but usually comprises the following phases:

- conceptual design (also called 'basic design' or 'basis of design');
- detailed design;
- construction;
- commissioning;
- hand-over.

Conceptual and detailed design phases are distinct parts of the design or planning phase.

Conceptual design aims at translating the user's requirements into functional, operational and performance requirements. It defines the containment concept, circulation schemes and the main technical options, e.g. with respect to air handling

and conditioning (HVAC) and decontamination means, and identifies the needs for equipment and utilities. It also provides the bases for an informed choice by the user when alternative options can be envisaged. The bases of a commissioning plan are normally drafted at this stage, together with the definition of the required performances. Conceptual design also includes more precise budget estimates and time tables than those proposed in the feasibility study.

Detailed design is the heavy engineering part, where all the concepts defined in the previous phase are fully developed into specifications and operational solutions in accordance with the desired performances. The definitive commissioning plan is normally developed at this stage. Budget estimates and time tables are consolidated. The specifications and narratives generated during the detailed design are used for the tender and for hiring the construction firm(s). They will of course also serve as the basis for the realisation of the construction according to the user's needs and the performance expectations set in the conceptual phase.

The construction phase is the most visible part of a project. It is normally realised under the supervision and with the technical support of the architect and engineering firm that has developed the design.

The commissioning phase is the phase where conformity with the specifications is verified. Commissioning usually consists in visual inspection as well as functional, operational and performance testing (also called qualification, or validation) of the most critical devices or systems according to the commissioning plan.

The hand-over corresponds to the contractual transfer of responsibility from the architect and engineering firm to the user, after acceptance of the facility by the user on the basis of the commissioning. It also corresponds to the launch of operations by the users. This phase should be preceded by a progressive familiarization of the users (scientific personnel and maintenance) to the new biocontainment facility, the establishment of adapted procedures and the operational training.

The design and construction of biocontainment facilities is a complex and arduous enterprise that is very often subject to difficulties and may sometimes end up in real failures, even for projects that have been assessed as viable. Termination of numbers of projects has been delayed, causing a delay in operations with often a high financial impact, while deficiencies in quality have impeded the optimal use of others, compromising the safety and/or sustainability of the operations.

Many of the technical problems that occur in the construction of biocontainment facilities deal with aspects that are more or less specific to containment or appear particularly sophisticated in biocontainment facilities (HVAC dimensioning and regulation, functioning of specific equipment like decontamination stations, quality of finishes…). Such problems may originate from deficiencies in the conceptual and detailed design phases or from poor realisation in the construction phase. They may be identified during the execution phase, but are more often revealed later in the project, in the best cases during the commissioning phase, otherwise, in case of deficient commissioning, when the facilities are in operation.

Some of the most frequently cited general reasons of failure in biocontainment construction projects are:

- a poor definition of the users needs and requirements;
- a poor understanding of the users needs by the architects and engineers;
- a lack of expertise in biocontainment and biorisk management (in general);
- a poor understanding of the technical aspects of containment by the users;
- a lack of specific experience of the architect and engineering firm in biocontainment;
- a lack of involvement of the user in the project;
- a lack of consultation of key users' representatives (key scientific personnel, biosafety professional, maintenance staff, quality assurance staff…);
- frequent or late changes in requirements by the users, together with a poor change management process;
- a lack of competencies and know-how of the construction firms;
- a lack of supervision of the execution;
- deficient checking and commissioning.

As it can be seen, many of the reasons are linked to a lack of expertise and competencies, together with difficulties of communication or understanding and project management issues.

Lack of expertise and experience is particularly damaging given the complexity, diversity and fast evolution of biological sciences and biological processes on one side, and the high technical complexity of biocontainment on the other side. Lack of specific experience in biocontainment is quite obvious nowadays. Indeed, given the high demand in biocontainment facilities, many architect and engineering offices as well as construction firms are entering this very specific market with limited or no experience. This is true in some economically developed countries (e.g. in Europe, where many of the firms that build containment facilities have experience in clean rooms and Good Manufacturing Practices (GMPs) but may have some trouble integrating the specific requirements of biosafety and biocontainment), and even more in many developing countries where technical resources in general are limited.

Linked to this, difficulties of communication and understanding arise from the fact that two different worlds, the world of scientists on one side and the world of architects and engineers on the other side, are associated in a project while they have different modes of functioning, different views, different interests and objectives, different high level expertises and different technical languages. This, together with the limited knowledge of the functioning of a construction project by scientists, contributes to the often insufficient involvement of the user and user's representatives in the project, while their input is crucial at different stages, starting with the conceptual design.

Project management problems can be diverse: lack of consulting, reporting or supervision, poor change management, deficient commissioning… Such problems

can remain unnoticed without effective control by the user or user's representatives. Architect and engineering firms are usually driven by strong budget and timing constraints, and may not be willing to expand their mission beyond a certain point without an appropriate challenge and control by the user.

A frequent problem that is independent from possible technical or project management problems is the delay in the launch of operations after the hand-over has taken place. The complexity of operating new biocontainment facilities for both the scientific and the maintenance staff is often underestimated by the user. In many cases, the effective take-over is too abrupt and the logistic preparation, the development of operational procedures and the personnel training occur much too late in the overall process.

The number and nature of the problems observed stress on the need for a real and strong commitment of the user, the engagement of ad hoc expertise and the setting of an efficient project management.

Given the importance of obtaining biocontainment facilities that correspond to their needs, the user institution shall ensure its full ownership of the project despite the fact that most if not all of the designing and constructing activities are contracted.

A first manner to ensure ownership is to delegate a qualified user's representative in the project team. The user's representative should be the privileged link between the architect and engineering team and the institution. He/she should not be involved in all the technical meetings, but should be kept informed of all the issues regarding the project, for instance on the basis of a weekly project management meeting with the project manager and the key actors of the moment. He/she should facilitate the communication both ways between the users and the project team. This connecting role of the user's representative is particularly crucial when several end users are going to share the new facilities, as it is often the case in research settings. The user's representative also contributes to bringing together key stakeholders (biosafety professional, security manager, quality manager, maintenance staff…) at various stages of the project, depending on the need and according to the interests of the institution. Given his/her pivotal role, the user's representative should be knowledgeable both in the operational activities and in the management of a design and construction project. He/she should have strong management and communication skills[113]. He/she should also be allowed the needed time and authority to accomplish his/her role.

A second way to ensure ownership of the project is to install a steering team that controls the project from the user's perspective. The control of the steering team should operate on the key aspects of the project, such as performance, timing and budget. Technical issues of relevance should also be treated. The steering team should be composed of a representative of the senior management of the institution, the heads of the concerned operational units, the user's representative, the project manager and possible ad hoc experts.

[113]Facility managers, biosafety officers, and scientists with a strong technical orientation have assumed the role of user's representative successively in major biocontainment projects.

In situations where lack of experience or knowledge in biocontainment or other key technical aspects may compromise the success of the project, it may be wise for the institution to set an independent technical review team with qualified internal and/or external consultants[114]. The role of this technical review team should be to act as a support to the user in ensuring that the technical issues are treated in an appropriate manner to guarantee operational efficiency and sustainability. Specifics of the mission of the technical review team can be to supervise third party commissioning and organise the activities related to the hand-over (development of procedures, training…). The team should report to the steering team and work in close relation with user's representative and possibly, depending on the context, with the architects and engineers of the design and engineering company.

Another element of importance for the success of a biocontainment construction project is the hiring of the design and engineering firm. Their main role is to complete the conceptual and detailed design, to manage the project and to supervise and control the execution of the construction. The design and engineering firm must have a good experience of managing projects with a similar level of complexity and have the technical skills required for the design and engineering of technically complex facilities. Project management skills can be transferred from other technically complex construction projects, as well as most of the technical knowledge associated to biocontainment measures (HVAC, utilities, finishing…). However, if technical competencies are transferred from other domains like pharmaceutical research or production for instance, there is an absolute need to ensure that the specifics of biorisk management are taken into account, for instance through the hiring of ad hoc experts.

The last element of success is the hiring of the construction firm(s). Building biocontainment facilities require mastering a number of specific construction and engineering techniques. In case these skills are not readily available locally, additional supervision and training of the concerned workforce must be planned in the project framework.

In any case and regardless of the experience and competencies of the construction firm, a good supervision and checking of the realisation needs to be done in real time during execution and after the completion of the construction, through the commissioning process. Checking and supervision during construction are generally a legal or a contractual part of the responsibilities of the architect and engineering company. Their checking activity could be completed by some additional, independent checking by the technical review team. This practice does not intend to replace the supervision and checking by the architect and engineering firm but to ensure checking is made with due diligence. The commissioning can be done either by the architect and engineering firm or by a third party commissioner under the supervision of the technical review team.

[114] Some organizations that support development projects in developing and emerging countries require an independent technical review team made of biosafety and other consultants with the required expertise for biocontainment construction projects.

In any case, the commissioning must be made according to a commissioning plan that has been developed during the design phase on the basis of the desired performances. The commissioning plan should be made available to the construction firm(s) during the hiring process, so that they know what exact performances are expected from them before they contract for the work.

Managing biorisks in operations

Current situation, gaps, and limitations

At least some level of biorisk management has become a legal obligation in a number of regions around the world (see Appendix B for more information on biorisk regulations). However, even in the developed world, there are quite a lot of countries where only biosafety is regulated and biosecurity regulations do not exist. Where biosafety regulations are in place, they sometimes appear quite incomplete. It is the case in many Asian countries where biosafety regulations only cover GMO-related activities in relation to the Cartagena protocol, without considering non-modified pathogens. There are also countries where some projects involving at risk biological activities take place that do not have any biosafety or biosecurity regulation at all.

Most regulations are based on a notification and authorization process that is based on some risk assessment. The level of risk assessment varies from a descriptive approach based on an almost automatic use of a biohazard classification of biological agents to a more complete hazard identification (of GMOS for instance) and a risk analysis of the related activities. The level of effective control by the authorities also varies from one region or country to another, reflecting socio-economic, cultural and political differences.

On the other hand, the required technical protection and prevention measures are based on universally recognized guidelines[115] and are therefore rather comparable from one area to another. This is at least true for the general concepts, but much less for the technical specifications that can be used to apply the concepts. Indeed, guidelines and regulations are generally not very prescriptive with respect to the technical ways to reach performance objectives. This may make their concrete implementation somewhat difficult but at least presents the advantage to allow developing measures that are fully adapted to the different situations, including in different local contexts.

The way individual organizations apply regulations and manage biorisk in practice is also extremely variable. As indicated in the survey made in the framework of this project, some organizations do not carry out any biorisk assessment at all, or do not have any structured and documented approach to do so. Moreover, while in some

[115] Mainly but not exclusively the WHO "Laboratory Biosafety Manual" (2004) (http://www.who.int/csr/resources/publications/biosafety/Biosafety7.pdf) and the "Biorisk Management: Biosecurity Guidance" (2006) (http://www.who.int/csr/resources/publications/biosafety/WHO_CDS_EPR_2006_6.pdf).

countries there might be some requirements for dynamic risk management[116] based on a risk assessment of the activities[117], many institutions still apply biosafety measures on a check-list mode or copy-pasting measures that may not be perfectly adapted to the concerned activities and actual level of risk. Possible results are an insufficient or exceeding level of protection, poorly managed technical problems, unjustified costs or a lax application of the prescribed measures, all difficulties which may one way or another appear as threats for the sustainability of the activities.

Another consequence of applying regulations on a check-list mode is that biosecurity aspects can be totally neglected by organizations that are operating in countries where there is no biosecurity regulation.

As highlighted earlier in this report, key challenges to managing biorisks include tools to monitor system effectiveness, lack of appropriate training and inadequate personnel reliability programs.

Required processes, knowledge, and skills

The process that is currently considered the most effective and efficient to manage risks and quality in an institution in a sustainable way is the management system approach. As noted earlier, the "Laboratory Biorisk Management Standard" CWA 15793[118] appears also as a way to introduce risk governance concepts in operational activities involving some level of biorisk. The standard applies the management system approach to biosafety and biosecurity. Depending on the relative importance of biorisk and other risks in an institution, CWA 15973 could be used either as a full standard against which certification should be achievable in the future, or as a guidance to integrate biorisk management into a more global risk or quality management program based on wider standards like OHSAS 18001 (occupational health and safety), ISO 14001 (environmental management) or ISO 9001 (quality management).

Managing biorisk at the level of an institution requires a wide range of knowledge: biology, microbiology, molecular biology, occupational health, laboratory animal sciences, technical aspects related to decontamination, biocontainment and other biosafety and biosecurity measures… Given their unique position in an institution and the fact they need to interact with a wide variety of stakeholders (laboratory personnel, laboratory heads, senior management, maintenance staff, health and safety managers, security staff, architects and engineers, public…), biosafety officers and other biosafety professionals also need strong management and communication skills. Although there is no universally recognised curriculum yet and the expertise that would be required in a given institution may depend on its activity (research, diagnostic, production…) and specific field of activities, initiatives are in place to recognize and certify biosafety professionals on the basis

[116] It is the way some European countries like Belgium have translated Directive 89/391/EEC in their legislation.
[117] See previous examples of references on the subject
[118] ftp://ftp.cenorm.be/PUBLIC/CWAs/wokrshop31/CWA15793.pdf.

of their training and experience in North America[119] and, more recently, to define the competence requirements for biosafety professionals in Europe[120].

The knowledge that is needed to run the biorisk management program in an institution also needs to be distributed transversally to the personnel and other stakeholders through training and information.

Available tools

As pointed out above, the "Laboratory Biorisk Management Standard" CWA 15793 provides a suitable basis to organize and manage biorisk in an effective and sustainable manner. It is based on a management system approach ("Plan - Do - Check -Act") that is compatible with other management systems. CWA 15793 sets the requirements necessary to control biorisk at institutional level, including with respect to the roles, responsibilities and authorities of the stakeholders. It implies compliance to national or local applicable regulations. Since the requirements of the standard are generic, not technical and intended to be applicable to all concerned institutions, CWA 15793 refers to other standards and guidelines, starting with the WHO central guidance documents on biosafety and biosecurity[121, 122], for their application.

Most of the preventive and protective measures to ensure the control of biorisk in the operational phase (the "do" phase) of the biorisk management system are available in existing regulatory and guidance documents. This is not necessarily the case for the biorisk assessment (part of the "planning" phase) and for the ways to measure and document the performances of the biorisk management program (the "checking" phase), for which some tools are still missing or not widely known and recognized.

The technical part of the risk assessment, especially the hazard identification, is sometimes well specified, as for instance for the risk assessment of GMOs in Europe where regulatory texts and guidance documents give procedures to carry out structured and documented risk assessments[123]. Things are much less precise to analyse the risk related to the activities. In this case, either a non-structured approach or tools that were developed in other domains of safety are used. Non-specific tools include risk assessment techniques like tree-based approaches or SWIFT analysis ("What if …?") for the activities themselves, and Hazard and Operability (HAZOP) or Safety Integrity Level (SIL) studies for equipment and associated processes. Well used, in a relevant context and with appropriate knowledge and experience, such general tools are likely to give good results when

[119] Registered Biosafety Professionals (RBP) and Certified Biological Safety Professionals (CBSP) programs (http://www.absa.org/biosafety.html).

[120] The Biosafety Professional Competence project (CEN Workshop 53) (http://www.cen.eu/cenorm/sectors/technicalcommitteesworkshops/workshops/ws53-bsp.asp / http://www.ebsaweb.eu/EBSA_Activities-p-185/Biosafety_Professional_Competence.html).

[121] See note 12.

[122] Guidance on the application of CWA 15793 may also be developed in the future.

[123] Bases for the risk assessment of genetically modified constructions are given in European Directive 90/219/EEC and further developed in national regulations or guidelines.

applied to biorisk. While some would benefit from being better adapted to biosafety and possibly biosecurity, their purpose, relevance, advantages and drawbacks when applied to biorisk issues should in general be better known and documented.

The same overall observations can be made for incident and accident investigation: general tools such as the causal tree (or root cause) analysis or the bow tie approach (which also allows identifying corrective actions) are available and useful, but they need to be used with the specific knowledge and experience of biorisk management.

Given the limitations of using statistics of incidents and accidents as performance indicators due to their relatively low occurrence, reporting of near-misses could be seen as a possible alternative. According to the accident pyramid model[124], their analysis could also be useful to adapt preventive and protective measures (in the "acting" phase). However, reporting of near-misses is arduous and difficult to organise, is only feasible in mature institutions with a good safety climate, and their interpretation is subject to caution. In many cases, setting the reporting of near-misses as a performance indicator and a management tool would not reveal cost-effective, except perhaps on the basis of a good selection and definition of what specific near-misses should be notified.

On the other hand, an inspection program that would detect and count non-compliance and non-conformities in a systematic way should provide useful performance indicators as well as a concrete basis to review and re-adjust the biorisk management program.

Tools in development like the BioRAM methodology[125] should also provide a way to measure the performance of biosafety and biosecurity management in an institution and to quantify, visualise and simulate the effects of changes in the biorisk control measures.

Finally, occasional third-party inspections and audits are also likely to provide an effective way to evaluate the overall performance of the biorisk management system and contribute to continuous improvement and sustainability.

CONCLUSIONS

Risk governance is emerging as a global, holistic approach to manage issues like scientific uncertainty or preparedness to natural disasters or major sociological or economical events as well as any situation that is submitted to risks that may impact an organization in a substantial way. The risk governance approach provides effectiveness and legitimacy to the risk management decision taking. Due to the complexity and diversity of biological processes and activities, and the multiplicity

[124]According to this classical safety model, there is a statistically-based ratio between the number of near-misses, minor incidents, accidents and serious or fatal accidents.
[125]See http://www.sandia.gov/ram/BIORAM.htm.

of the risks associated to these processes and activities, biorisk management should certainly benefit from the precepts of risk governance.

APPENDIX A – BIORISK CASES

The 63 biorisk cases summarized below are limited to occurrences that are recent, publicly available, and from sources that can be verified or are considered authoritative. North America (52 cases) is the most heavily represented in the examples, followed by Europe and Russia (8 cases) and then Asia (3 cases). The sectors represented are also not evenly distributed: 47 examples from academia, 9 from government-affiliated institutions, 4 involved private organizations, and 2 at hospitals. This breakdown in clearly not representative for many reasons, including that the public sector is more transparent by design.

Laboratory Exposure (actual or potential)

Example 1[126]

An occupational exposure by a technician to *Brucella* occurred in a laboratory at Texas A&M University in College Station, Texas in February of 2006. The exposure was not immediately reported to the Division of Select Agents and Toxins (DSAT) of the CDC and a written report was not submitted within seven days, as required by law. DSAT was only notified in April of 2007. Furthermore, the locale where the exposure occurred was not approved by DSAT to conduct *Brucella* at the time.

Example 2[127]

A local outbreak of tularemia in researchers in Boston University (BU) occurred in 2004. Serology on three researchers working on the vaccine strain (LVS) of *Francisella tularensis* returned positive; all three also reported clinical symptoms of tularemia during the year in question. Tests on laboratory LVS samples revealed contamination with Type A *F. tularensis*, a wild-type virulent strain classified as a US select agent. This contamination likely resulted in the incidents of illness. Review of the BU biosafety program, including lab practices and medical surveillance protocols, revealed important deficiencies. However, the source of the contamination itself is unknown, and could have occurred prior to samples arriving at BU.

Example 3[128]

In 2004, a researcher at the US Army Medical Research Institute of Infectious Diseases working in Biosafety Level 4 containment received a needle-prick while using a syringe on mice infected with a mouse-adapted variant of Ebola Zaire. The syringe had been used on mice which had been challenged 2 days prior with the virus. Standard biosafety procedures were followed throughout, including the isolation of the researcher in a medical containment suite. Eventually neither the

[126]from DSAT Director to Responsible Official, Texas A&M University, April 20, 2007

[127] M. Anita Barry, Report of Pneumonic Plague in Three Boston University Researchers, March 28, 2005.

[128]Mark G. Kortepeter et al, Managing Potential Laboratory Exposure to Ebola Virus by Using a Patient Biocontainment Care Unit, Emerging Infectious Diseases, 14(6), June 2008.

researcher nor the mice developed symptoms of Ebola or seroconverted, and the researcher was released from containment after 21 days.

Example 4[129]
A researcher at the University of New Mexico was reportedly "jabbed with an anthrax-laden needle" in 2004.

Example 5[130]
A researcher at the University of New Mexico reportedly "experienced a needle stick with an unidentified pathogenic agent that had been genetically engineered" in 2005.

Example 6[131]
A researcher at the Medical University of Ohio was reportedly "infected with Valley Fever (*C. immitis*)" in 2004.

Example 7[132]
One or more workers at the Medical University of Ohio were reportedly exposed to an aerosol of *C. immitis* after a laboratory accident in 2005.

Example 8[133]
A worker at the University of Chicago in 2005 reportedly "punctured his or her skin with an infected instrument bearing a BSL-3 select agent. It was likely a needle contaminated with either anthrax or plague."

Example 9[134]
A researcher at the Bernard Nocht Institute for Tropical Medicine in Hamburg, Germany accidently pricked herself with a needle while working with Ebola virus in 2009. An experimental vaccine was flown to Germany from Canada and administered 40 hours after exposure. The researcher recovered.

Example 10[135]
A researcher at the State Research Center of Virology and Biotechnology (also known as Vector) in Russia died in May of 2004 after pricking herself with a

[129] The Sunshine Project News Release, Texas A&M Bioweapons Accidents More the Norm than the Exception, July 3, 2007
[130]The Sunshine Project News Release, Texas A&M Bioweapons Accidents More the Norm than the Exception, July 3, 2007
[131] The Sunshine Project News Release, Texas A&M Bioweapons Accidents More the Norm than the Exception, July 3, 2007
[132] The Sunshine Project News Release, Texas A&M Bioweapons Accidents More the Norm than the Exception, July 3, 2007
[133] The Sunshine Project News Release, Texas A&M Bioweapons Accidents More the Norm than the Exception, July 3, 2007
[134] The Canadian Press, Canadian-made Ebola vaccine used after German lab accident, March 20, 2009
[135] The New York Times, Russian Scientist Dies in Ebola Accident at Former Weapons Lab, May 25, 2004. http://www.nytimes.com/2004/05/25/international/europe/25ebol.html

needle laden with the Ebola virus. The laboratory did not inform the World Health Organization until several weeks after exposure. The researcher was apparently working on a vaccine for Ebola.

Example 11[136]

A worker in a laboratory at AFSSA in France in 2009 potentially exposed herself and fellow laboratory workers to anthrax by opening 6 vials of biological material in a Level 2 laboratory biosafety cabinet immediately after a heat-inactivation procedure. The technician had not verified that the heat-inactivation process had actually worked. Although "the exposure, if any, was trivial", personnel in the laboratory "were given antibiotics." It was unclear whether the verification procedure, which involved plating samples from the heat-inactivated vials on sheep blood agar and observing growth after 24 hours, yielded positive results.

Example 12[137]

In September of 2003, a doctoral student in Singapore contracted SARS after working with contaminated West Nile Virus samples in a Level 3 laboratory. While following correct safety procedures for West Nile, the possibility of cross-contamination of samples had not been taken seriously and appropriate procedures for work with aerosol-transmitted SARS virus were not in place. Insufficient training, inappropriate record keeping and a lack of a culture of safety were identified as root causes.

Example 13[138]

In December of 2003, a researcher at the National Defense University in Taipei, Taiwan contracted SARS after following incorrect spill decontamination procedures inside a Biosafety Level 4 laboratory. Non-specific symptoms were noted for several days before a visit to the hospital led to a confirmation of SARS infection. No secondary infections occurred.

Example 14[139]

Two laboratory workers in the National Institute of Virology in Beijing contracted SARS between March and May of 2004 after working with improperly inactivated virus. Investigators expressed " serious concern about biosafety procedures at the Institute – including how and where procedures using SARS coronavirus were carried out, and how and where SARS coronavirus samples were stored." Concern was also expressed at the time over the large number of samples collected from humans and animals during the 2003 epidemic and stored in various laboratories around the world.

---

[136] ProMed, Anthrax, Laboratory Exposure - France, March 30, 2009

[137] Singapore Ministry of Health Review Panel, Biosafety and SARS Incident in Singapore September 2003

[138] Singapore Ministry of Health Review Panel, Biosafety and SARS Incident in Singapore September 2003

[139] CDC Health Advisory, Severe Acute Respiratory Syndrome (SARS) in Taiwan, Dec 17, 2003

Example 15[140]

Four laboratory technicians at the Valme University Hospital in Seville, Spain were diagnosed with acute brucellosis in 1988 after working with blood cultures of the organism. Serology and culture from all four patients indicated infection with *Brucella melitensis* bio-type 1. No other persons in the laboratory were infected. Review of events and procedures indicated that no extraordinary incidents had occurred and that culture samples were handled correctly except for the fact that a biological safety cabinet was not used. Thus, it was suggested that the route of exposure were aerosols generated by standard laboratory procedures. The lab modified its protocols to require the work to be conducted with safety cabinets and to emphasize the importance of good laboratory techniques and the dangers of aerosolization.

Example 16[141]

In 2001, the New England Journal of Medicine published a case report of glanders in a 33-year old microbiologist working on *Burkholderia mallei* at the US Army Medical Research Institute of Infectious Diseases in Frederick, Maryland. The researcher did not routinely wear latex gloves and exposed skin was implied to be the means of infection. Illness persisted and grew more severe after several months and treatment was complicated by the lack of clinical experience with glanders, as this was the first human case in the United States in over 50 years.

Example 17[142]

Six of nineteen medical technologists and none of three medical technology students working in a clinical microbiology laboratory in Rhode Island were infected and became ill with *Shigella sonnei* in January of 1996. Study of the cultured isolates indicated that the *Shigella* strain in question was nearly identical to a control strain kept by the laboratory and which was in use at the time of exposure by one of the unaffected medical technology students. The student was the only member of the laboratory to routinely wear gloves. However, he did not follow other laboratory protocols, including the use of a separate processing sink for disposal of work samples. Instead, he utilized a closer hand-washing sink, and this apparently led to the contamination of the work area with *S. sonnei* which in turn infected others who used the sink's faucet handles. Strict surveillance of laboratory activities, including use of gloves and proper sinks, the installation of foot or infrared faucet controls rather than handles, and the use of strains other than active pathogenic ones for teaching lab procedures to medical technology students were identified as necessary mitigating measures.

---

[140]E. Martin-Mazuelos et al, Outbreak of *Brucella melintensis* among Microbiology Laboratory Workers, Journal of Clinical Microbiology, 32(8), pp. 2035-2036, 1994.

[141]A. Srinivansan et al, Glanders in a Military Research Microbiologist, The New England Journal of Medicine, 345(4), pp. 256-258, 2001.

[142] L. A. Mermel et al, Outbreak of *Shigella sonnei* in a Clinical Microbiology Laboratory, Journal of Clinical Microbiology, 35(12), pp. 3163-3165, 1997.

Unintentional Release from Facility

Example 19[143]

The likely release of Foot and Mouth Disease virus into the environment occurred from a laboratory in the village of Pirbright in the United Kingdom, resulting in a local outbreak of the disease in August of 2007. The accidental release was determined likely to be a result of improper liquid waste disposal as a result of the deteriorated condition of the site drainage system. A review of compliance with general procedures also highlighted a failure to maintain complete records of human movement in and out of the facility, and otherwise poor monitoring and access controls.

Example 20[144]

In Vladivostok, Russia in 2000, eight children ages 11-14 became ill after playing with discarded smallpox vaccine vials. The cause was most likely improper decontamination and disposal procedures by a nearby public health station.

Theft

Example 21: Theft[145]

A former researcher at the National Microbiology Laboratory in Winnipeg, Canada stole 22 vials of Ebola virus genetic material which was discovered as he attempted to cross the US-Canada border in May of 2009. The material was not infectious and thus posed no public health risk. The researcher claimed he did not want to start his research "from scratch" at a new job with the US National Institutes of Health.

Example 22[146]

In 2001, a researcher at the US Army Medical Research Institute of Infectious Diseases (USAMRIID), Bruce Ivins, is suspected of having mailed several letters containing anthrax spores through the US Postal Service to various recipients across the United States. The mailings resulted in the deaths of five people and the sickening of 17 others. The spores were believed to have been taken from USAMRIID. The motivation seems to have been to draw attention to the threat of bioterrorism in order to promote the biodefense cause broadly, and more specifically, to promote the anthrax work and vaccine Ivins was involved in developing.

Example 23[147]

---

[143] Health and Safety Executive, Final report on potential breaches of biosecurity at the Pirbright site 2007, December 20, 2007

[144] K. B. Byers, Biosafety tips. Applied Biosafety 14(2) , pp. 99-102, 2009.

[145] CBC News, Winnipeg researcher charged with smuggling Ebola material into U.S., May 13, 2009. http://www.cbc.ca/health/story/2009/05/13/border-biological-agents.html

[146] http://www.fbi.gov/anthrax/amerithraxlinks.htm

[147]The New York Times, Ex-Medical Technician Is Held Without Bail in Hepatitis C Outbreak in Colorado, July 9, 2009. http://www.nytimes.com/2009/07/10/us/10denver.html

A former surgical technician in Colorado was charged in 2009 of stealing drugs loaded in syringes from her places of work and replacing the syringes with saline solution. Some of the saline syringes had been previously used by her, posing a risk that she spread her hepatitis C infection to patients in the hospitals where she worked. Despite the fact she claimed she did not know she was infected until after developing illness during the investigation, blood testing shown to her prior to employment at one of the hospitals demonstrated the presence of antibodies to the virus. Although it does not seem there was malicious intent to spread infection. Investigators are determining the extent, if any, of hepatitis C infection resulting from the technician's actions.

Inappropriate Shipments

Example 24[148]

The University of California at Berkeley in 2005 reportedly "received dozens of samples of what it thought was a relatively harmless organism. In fact, the samples contained Rocky Mountain Spotted Fever. As a result, the samples were handled without adequate safety precautions, until the mistake was discovered. Unlike nearby Oakland Children's Hospital, which previously experienced an anthrax mix-up, UC Berkeley never told the community."

Example 25[149]

Improperly heat-inactivated samples of *Bacillus anthracis* were sent to a laboratory in Oakland Children's Hospital in 2004 resulting in the possible exposure of seven laboratory workers. The samples were twice tested for activity by culture, once before shipment, and again upon arrival at the laboratory. Both results were negative. Sub-culturing of samples was not attempted. Infectivity was discovered when 49 of 50 mice inoculated with the samples as part of a vaccine experiment died quickly. The possible emergence of a heat-resistant variant of *B. anthracis* was suggested.

Example 26[150]

Samples of H3N2 human influenza virus shipped from a Baxter International plant in Austria to an Austrian research company were found to be contaminated with live H5N1 avian influenza virus. The contamination was discovered when a subcontractor of the Austrian research company in the Czech Republic inoculated ferrets with the viral samples and the ferrets died. Subcontractors in Germany and Slovenia also received contaminated samples. The situation was particularly worrisome as the comingling of human and avian viruses in a host could produce a hybrid strain through the process of reassortment which could in turn increase the potential for a pandemic. Baxter International "called the mistake the result of a

[148] The Sunshine Project News Release, Texas A&M Bioweapons Accidents More the Norm than the Exception, July 3, 2007

[149] The Scientist, US lab is sent live anthrax, June 11, 2004. http://cmbi.bjmu.edu.cn/news/0406/54.htm

[150] Science Magazine, Company Mum on Details of Flu Virus Mishap, March 18, 2009. http://blogs.sciencemag.org/scienceinsider/2009/03/company-mum-on.html

combination of 'just the process itself, (and) technical and human error in this procedure.'"

Example 27[151]

Ipsen Limited, a pharmaceutical company based in France, was accused in a Washington Times editorial in 2009 of aiding Iran's biological weapons capacity by selling medicinal products based on botulinum toxin to the University of Tehran and the Pasteur Institute of Iran.

Example 28[152]

EMD Biosciences Inc, a California company, settled charges in 2005 of exporting biological toxins to Canada without proper Department of Commerce licenses. The licensing requirements are in place as part of export control policies intended to regulate the proliferation of chemical and biological weapons under Australia Group agreements. EMD's 134 violations were alleged to have occurred between June 2002 and July 2003, and followed similar charges and a settlement in 1999 involving the previous incarnation of the company for 171 unlicensed shipments of toxins between 1992 and 1994. The Department of Commerce's Bureau of Industry and Security was responsible for the charges and the settlement.

Example 29[153]

CN Biosciences Inc, a California company, settled charges in 1999 of 171 violations of export control law related to the shipment outside of the United States of restricted biological toxins. The violations were alleged to have occurred between July 1992 and January 1994 and were associated with various foreign destinations. These cases preceded a second settlement in 2005 by the successor company to CN, EMD Biosciences, for similar violations.

Inventory Discrepancies

Example 30 [154]

During the general inspection of Texas A&M University in 2007 by the CDC, it was discovered that 3 vials of a select agent, *Brucella abortus*, were missing from the strain collection of a former researcher and remained unaccounted for. Furthermore, reviewing the researcher's inventory, it was found it did not fully meet applicable regulatory requirements. Other researchers had poorly organized inventory records that did not always match with actual stocks and were difficult to manage.

---

[151] Washington Times, Editorial: The Ipsen-Iran Connection, May 3, 2009.
http://www.washingtontimes.com/news/2009/may/03/the-ipsen-iran-connection/

[152] Bureau of Industry and Security, California Biotech Firm Settles Charges of Unlicensed Exports of Biological Toxins, May 11, 2005.
http://www.bis.doc.gov/news/2005/emdbiosciences.htm

[153] Bureau of Industry and Security, California Biotech Firm Settles Charges of Unlicensed Exports of Biological Toxins, May 11, 2005.
http://www.bis.doc.gov/news/2005/emdbiosciences.htm

[154] Letter from DSAT Director to Responsible Official, Texas A&M University, August 31, 2007

Example 31[155]

An institution-wide inventory at the US Army Medical Research Institute of Infectious Diseases in 2009 resulted in the discovery of more than 9,200 unrecorded disease samples. The vast majority seem to have been "working stock accumulated by researchers over several decades", and the discrepancy over documented and unaccounted samples seems to have arisen because of the way the sample database was created in 2005, which required current researchers to account for their samples but ignored what may have been stored by previous researchers. About half of the newly discovered samples were deemed worthless from a scientific perspective and were destroyed. Yearly inventory audits will now be conducted.

Example 32[156]

In December of 2008, a laboratory at the University of Medicine and Dentistry in Newark, New Jersey was unable to account for a bag with two dead frozen mice that had been infected with *Yersinia pestis*. The bag was stored in a locked freezer, and was to be sterilized and incinerated along with a series of other samples. The laboratory notified the CDC, FBI and state officials, and foul play was ruled out. The likely explanation seems to have been a bag getting stuck to another bag as a result of the freezing process. Protocols have been amended as a result "to inventory all logged hazardous waste bags prior to sterilization."

Example 33[157]

In September of 2005, a laboratory at the University of Medicine and Dentistry in Newark, New Jersey found three live mice infected with *Yersinia pestis* missing from separate cages. Officials concluded that the mice probably died.

Unauthorized Access

Example 34[158]

Texas A&M University was cited in 2007 by the CDC for at least seven incidents of unauthorized access to select agents. Researchers involved were repeatedly granted access to restricted areas and conducted restricted experiments prior to receiving necessary regulatory approval.

Example 35[159]

Eight State, local, private and commercial laboratories working with select agents were reviewed by the CDC in the United States between November 2003 and September 2005. Of these, three "had weaknesses in access controls. Two of these

[155] Frederick News Post, USAMRIID finds 9,200 disease samples it didn't know it had, June 18, 2009.
[156] NJ.com, UMDNJ facility loses two plague-infected dead lab mice, Feb 07, 2009. http://www.nj.com/news/index.ssf/2009/02/dead_lab_mice_lost_from_umdnj.html
[157] The Seattle Times, 3 plague-infected lab mice missing, Sep 16, 2005. http://seattletimes.nwsource.com/html/nationworld/2002498338_plague16.html
[158] Letter from DSAT Director to Responsible Official, Texas A&M University, August 31, 2007
[159] Department of Health and Human Services Office of Inspector General, Summary Report on Universities' Compliance With Select Agent Regulations, June 30, 2006

entities had allowed an unapproved individual to accept and handle select agent packages. The third entity had authorized an unapproved individual to access select agents."

Unauthorized Experiments

Example 36[160]

During a general inspection of Texas A&M University in 2007, the CDC cited the university for failure by its Responsible Official, as defined by select agent regulations, to inform the CDC's Division of Select Agents and Toxins of a series of restricted aerosolization experiments with *Coxiella burnetii* on nine occasions from May of 2003 to June of 2005. These were conducted prior to DSAT approval of the principal investigator's work, which occurred October of 2005.

Inadequate Biosafety Measures

Example 37[161]

Texas A&M University was cited in 2007 by the CDC for lack of proper primary containment barriers between its Madison Aerosol Chamber and laboratory areas, as required by regulation. "Administrative controls in place to prevent workers from being exposed to biohazards were not adequate. Standard operating procedures were not available to address animal handling or maintenance procedures for laboratory workers using the Madison Aerosol Chamber. In addition, laboratory workers did not know how to determine that the unit was functioning properly or what routine maintenance was required."

Example 38 [162]

In Texas A&M University, large animal carcasses were "sectioned, double-bagged in plastic, sprayed with disinfectant, and passed through a thirty inch square opening for transport by truck or front end loader to the incinerator located approximately one mile away". Carcasses were thus not autoclaved as recommended prior to incineration or before leaving the facility. In addition, the effectiveness of contact times with disinfectant had not been determined nor was there a standard operating procedure to handle potential spills during the transport of waste.

Example 39 [163]

In Texas A&M University, there was a lack of appropriate biosafety controls. Personnel were often observed not to wear lab coats and other personnel protective equipment in areas where it was required, where otherwise unknowledgeable, ill-trained and unsupervised, and facilities were not properly maintained. Responsible officers did not seem in control of biosafety issues.

Example 40[164]

[160] Letter from DSAT Director to Responsible Official, Texas A&M University, August 31, 2007
[161]Letter from DSAT Director to Responsible Official, Texas A&M University, August 31, 2007
[162] Letter from DSAT Director to Responsible Official, Texas A&M University, August 31, 2007
[163]Letter from DSAT Director to Responsible Official, Texas A&M University, August 31, 2007

In Texas A&M University, there were repeated instances of failure in biosafety containment. Facilities were operated without necessary containment equipment, including functioning or properly maintained biosafety cabinets, autoclaves, and air handling systems. Animal waste disposal was not handled with appropriate containment in mind. Select agent aerosolization experiments were repeatedly carried out without primary containment barriers.

Example 41[165]

In Texas A&M University, there was a lack of operational and procedural select agent containment safeguards during particular experiments. For example, "inspectors noted that the biosafety procedures used in" a particular room "are not sufficient to contain the select agents. Specifically, information derived from laboratorian interviews revealed that the procedures employed during *Coxiella* aerosolization experiments" in a particular room "did not employ primary containment barriers. Although present practices designate the use of PPE, past history has demonstrated that the risk of exposure is still sufficiently high to warrant the use of primary containment barriers during the aerosolization experiments in question, and also during subsequent decontamination of all equipment employed".

Example 42[166]

Texas A&M University was cited in 2007 by the CDC for failing to enforce proper medical entry requirements for persons with access to select agents. Workers were allowed entry into restricted areas without appropriate respirator equipment or fit-testing, and without being educated as to the potential hazards of certain areas.

Example 43[167]

Texas A&M University was cited in 2007 by the CDC for a lack of an "effective medical surveillance program that was appropriate for work with select agents and toxins". For example, baseline titers were not kept as recommended or as stipulated in the institutions own protocols. In addition, inspectors determined that although it was known that 17% of personnel with contact with *Coxiella burnetii* had elevated antibody titers to the bacterium, there was no coordinated response or biosafety assessment as a result and no instructions for lab personnel to seek evaluation at Occupational Health. In a further example, there was no record of personnel working with *Brucella abortus, Brucella melitensis,* or *Brucella suis* receiving appropriate antibody testing as per the institution's medical surveillance plan.

Inadequate Biosecurity Measures

Example 44[168]

---

[164] Letter from DSAT Director to Responsible Official, Texas A&M University, August 31, 2007
[165] Letter from DSAT Director to Responsible Official, Texas A&M University, August 31, 2007
[166] Letter from DSAT Director to Responsible Official, Texas A&M University, August 31, 2007
[167] Letter from DSAT Director to Responsible Official, Texas A&M University, August 31, 2007

Six of fifteen universities reviewed for compliance of Select Agent regulations in the United States between November 2003 and November 2004 "had weaknesses in access controls, including procedures for issuing electronic access keys to select agent areas."

Example 45[169]
Eleven universities reviewed by the CDC for select agent security during 2002 and 2003 were found to have "physical security weaknesses" that "left select agents vulnerable to theft or loss, thus elevating the risk of public exposure."

Example 46[170]
At least half of eleven universities reviewed by the CDC for select agent security during 2002 and 2003 were found to have "inadequate procedures to identify persons barred from accessing select agents under the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001."

Example 47[171]
Out of eleven reviewed by the CDC for select agent security during 2002 and 2003, five used information technology resources for select agent data. All five were found to exhibit "control weaknesses that could compromise the security and integrity of the data."

Problems with Documentation

Example 48[172]
Texas A&M University was cited by the CDC in 2007 for failure to file proper personnel registration documents, specifically amendments to approved certificates of registration, with the CDC's Division of Select Agents and Toxins. Specifically, a Principal Investigator approved in the certificate of registration was no longer employed at the University. Also, as referred to in Example 2, a researcher was conducting experiments with a select agent several years prior to being approved in the certificate of registration for said experiments.

Example 49 [173]
During a general inspection by the CDC in 2007, Texas A&M University was cited for failing to develop a security plan that "has been designed according to a site-specific security risk assessment. In addition, security plans did not adequately

[168]Department of Health and Human Services Office of Inspector General, Summary Report on Universities' Compliance With Select Agent Regulations, June 30, 2006
[169] Department of Health and Human Services Office of Inspector General, Summary Report on Universities' Compliance With Select Agent Regulations, June 30, 2006
[170] Department of Health and Human Services Office of Inspector General, Summary Report on Universities' Compliance With Select Agent Regulations, June 30, 2006
[171] Department of Health and Human Services Office of Inspector General, Summary Report on Universities' Compliance With Select Agent Regulations, June 30, 2006
[172] Letter from DSAT Director to Responsible Official, Texas A&M University, August 31, 2007
[173] Letter from DSAT Director to Responsible Official, Texas A&M University, August 31, 2007

address procedures for moving select agents and toxins from one building to another. "

Example 50 [174]
During the general inspection of Texas A&M University in 2007 by the CDC, it was found there was a lack of access records to specific laboratory rooms that handled select agents.

Example 51 [175]
During the general inspection of Texas A&M University in 2007 by the CDC, it was found that the list of approved individuals under the select agent certificate of registration did not match the list of individuals provided by the university, indicating faulty record keeping and possibly leading to access being granted to unregistered personnel.

Example 52 [176]
Eight of fifteen universities reviewed for compliance of Select Agent regulations in the United States between November 2003 and November 2004 were found to be deficient "in their inventory and/or access records. Some inventory records contained incomplete user names or were difficult to decipher. Access records did not always identify individuals who had entered select agent areas or the dates and times of access."

Example 53 [177]
Six of fifteen universities reviewed for compliance of Select Agent regulations in the United States between November 2003 and November 2004 "had weaknesses in their security plans. In four cases, the universities had not used a systematic approach to identify threats or had not identified all relevant threats."

Example 54 [178]
Three of fifteen universities reviewed for compliance of Select Agent regulations in the United States between November 2003 and November 2004 had emergency response plans that "did not address one or more required areas."

Example 55 [179]
Eleven universities reviewed by the CDC for select agent security during 2002 and 2003 were found to have "inadequate inventory and recordkeeping procedures" that

[174] Letter from DSAT Director to Responsible Official, Texas A&M University, August 31, 2007
[175] Letter from DSAT Director to Responsible Official, Texas A&M University, August 31, 2007
[176] Department of Health and Human Services Office of Inspector General, Summary Report on Universities' Compliance With Select Agent Regulations, June 30, 2006
[177] Department of Health and Human Services Office of Inspector General, Summary Report on Universities' Compliance With Select Agent Regulations, June 30, 2006
[178] Department of Health and Human Services Office of Inspector General, Summary Report on Universities' Compliance With Select Agent Regulations, June 30, 2006
[179] Department of Health and Human Services Office of Inspector General, Summary Report on Universities' Compliance With Select Agent Regulations, June 30, 2006

prevented the reviewing agency "from concluding that the universities had complied with select agent transfer requirements."

Example 56[180]
Eight State, local, private and commercial laboratories working with select agents were reviewed by the CDC in the United States between November 2003 and September 2005. Of these, four "had incomplete inventory or access records."

Example 57[181]
Eight State, local, private and commercial laboratories working with select agents were reviewed by the CDC in the United States between November 2003 and September 2005. Of these, five had security plans that "did not meet one or more of the regulatory requirements. Three of these entitities' security plans were not sufficient to safeguard select agents and/or were missing required policies and procedures. One entity had not fully implemented its security plan controls."

Example 58[182]
Eight State, local, private and commercial laboratories working with select agents were reviewed by the CDC in the United States between November 2003 and September 2005. Of these, four "had not documented select agent training as required. The entities' records did not document that all approved individuals or visitors had received the necessary training or the means used to verify that individuals understood the training."

Example 59[183]
Eight State, local, private and commercial laboratories working with select agents were reviewed by the CDC in the United States between November 2003 and September 2005. Of these, three has incident response plans that "did not contain all required elements."

Inadequate Training

Example 60[184]
During a general inspection of Texas A&M University by the CDC in 2007, it was found that safety, security and incident response plans for laboratories were unfinished, were not reviewed nor revised as necessary every year, and procedures were not drilled or exercised every year as required by regulation.

Example 61[185]

[180] Department of Health and Human Services Office of Inspector General, Summary Report on Universities' Compliance With Select Agent Regulations, June 30, 2006
[181] Department of Health and Human Services Office of Inspector General, Summary Report on Universities' Compliance With Select Agent Regulations, June 30, 2006
[182] Department of Health and Human Services Office of Inspector General, Summary Report on Universities' Compliance With Select Agent Regulations, June 30, 2006
[183] Department of Health and Human Services Office of Inspector General, Summary Report on Universities' Compliance With Select Agent Regulations, June 30, 2006
[184]Letter from DSAT Director to Responsible Official, Texas A&M University, August 31, 2007

Texas A&M University in 2007 was found to have a lack of training records "for individuals approved to perform select agent activities", "no documentation provided that a formal training program had been established for all personnel that work in laboratories", and for the training that did occur, it did "not address the particular needs of the individual, the work they will do, and the risks posed by select agents and toxins." Safety lapses and inconsistencies in procedural behavior observed by inspectors were presented as evidence of an ineffectual biosafety training program.

Example 62[186]

Texas A&M University was cited in 2007 by the CDC for a comprehensive lack of adequate biosafety education for personnel. Workers interviewed were found to be unaware of potential hazards present in their work places, be they from biological or chemical agents in use. Personnel were also unaware of mitigation methods and procedures for those risks.

Example 63[187]

Three of fifteen universities reviewed for compliance of Select Agent regulations in the United States between November 2003 and November 2004 "had not provided training to one or more individuals with access to select agents or had not documented the means used to verify that individuals understood the training."

[185] Letter from DSAT Director to Responsible Official, Texas A&M University, August 31, 2007
[186] Letter from DSAT Director to Responsible Official, Texas A&M University, August 31, 2007
[187] Department of Health and Human Services Office of Inspector General, Summary Report on Universities' Compliance With Select Agent Regulations, June 30, 2006

APPENDIX B – BIOSECURITY REGULATIONS

To date, only a few countries have regulations specifically requiring security of dangerous pathogens and toxins. This list is not necessarily comprehensive but it covers those biosecurity regulations with which we are familiar. We hope that this section will be useful to orient individuals to the different biosecurity regulatory models. Although countries address biosafety through a spectrum of models, ranging from guidance documents and best practices to binding regulations, this section does not cover those, primarily because biosafety is a more established discipline.

Australia:
Legal framework: National Health Security Act
Year adopted: 2007
Scope: Human, zoonotic, and animal pathogens and toxins
Requirements: The regulated biological agents ("Security Sensitive Biological Agents (SSBAs) are divided into two tiers based on risk. All facilities with SSBAs must register with the government and designate a responsible official and deputy. The regulation articulates minimum requirements for risk assessment and the subsequent security measures put in place are to be based on the results of the risk assessment and the tier of SSBA. Facilities must meet specified inventory requirements, have written security plans, and conduct internal inspections at mandatory intervals.
Pending regulatory updates: An amendment to the act is currently being drafted (2009).

Canada:
Legal framework: Human Pathogens and Toxins Act
Year adopted: 2009
Scope: Human and zoonotic pathogens
Requirements: This Act controls and tracks the use of human pathogens and requires security. Facilities must be licensed. Individuals will need security clearances to have access to Risk Group 3 and 4 human pathogens and prescribed toxins.

Denmark:
Legal framework: Law 69 – Act on Securing Certain Biological Agents, Delivery Systems and Related Material
Year adopted: June 2008, effective November 2009
Scope: Human and zoonotic pathogens
Requirements: Facilities must designate a point of contact and be approved by the regulatory authority. Facilities must submit a written security plan that includes a vulnerability assessment. The institutional point of contact must pass a criminal background check.
Pending regulatory updates:

Japan:
Legal framework: Infectious Disease Control Law
Year adopted: 2006
Scope: Human and zoonotic pathogens and toxins
Requirements: The regulation sub-divides the regulated agents into four tiers. Tier 1 agents are deemed the highest risk and facilities are prohibited to posses these agents unless designated by the Minister of Health. Facilities must receive prior permission of the Ministry of Health to work with or posses these agents in Tier 2. Facilities must register with the Ministry if they have Tier 3 agents and, for Tier 4 agents, they must report any losses, thefts, or releases of those agents. For all tiers, facilities must implement minimum standards of laboratory biosafety and biosecurity based on risk assessment. And, all facilities are subject to government inspections.
Pending regulatory updates: Unknown

Singapore:
Legal framework: Biological Agents and Toxins Act
Year adopted: 2005
Scope: Human, zoonotic, and animal pathogens and toxins
Requirements: This act addresses possession, use, import, export, transfer, transport, and biosafety of listed agents. Violators can be subject to fines up to $1 million dollars and life imprisonment.
Pending regulatory updates:

United Kingdom:
Legal framework: Anti-Terrorism, Crime and Security Act of 2001
Year adopted: 2001
Scope: Human, zoonotic, and animal pathogens and toxins
Requirements: Part 6 of the Act was amended to regulate transfers of biological materials and Part 7 established security requirements for pathogens and toxins.
Pending regulatory updates:

United States:
Legal framework: The Bioterrorism Preparedness Act of 2002[188] and the USA PATRIOT Act are the governing legislation; the implementing Codes of Federal Regulation (CFR) are: 7 CFR Part 331, 9 CFR Part 121, and 42 CFR Part Year adopted: Interim CFRs issued in 2003; Final rules adopted in 2005
Scope: Human, zoonotic, animal, and plant pathogens and toxins ("select agents")
Requirements:[189] All facilities must register with the government and be subject to an inspection prior to being approved to posses select agents. Each facility must designate a responsible official and an alternate. Facilities must limit access to authorized individuals that must pass screening by the Department of Justice before being approved for access. The implemented security must be based on a facility-

[188]US Public Law 107-188
[189]www.selectagents.gov

specific risk assessment. The regulations also require facilities to have written biosecurity, biosafety, and incident response plans, meet specific inventory requirements, and provide training to everyone.
Pending regulatory updates: Legislation is pending in Congress to reauthorize the Select agent program and to strength the biosecurity requirements for some select agents (Lieberman-Collins bill).

APPENDIX C – BIORAM MODEL

Biosecurity Model for Persons and Animals in Area of Attack

This covers the biosecurity risks for theft from a facility and subsequent misuse against people (1a, 1b) and, with different weights, animals (1g, 1h). The weights have been elicited from biosecurity, security, and bioterrorism experts at Sandia National Laboratories. There are separate weights for the facility vulnerability criteria for each category of adversary (insiders and outsiders).

1. **Likelihood agent can be used as a weapon**
    a. Agent Properties
        i. Route of infection
            1. Inhalation
            2. Ingestion
            3. Percutaneous
            4. Contact
            5. Vector-borne
        ii. Infectious dose
            1. Inhalation
            2. Ingestion
            3. Percutaneous
            4. Contact
            5. Vector-borne
        iii. Stability outside of the host
        iv. Awareness of agent's BW potential
    b. Production and dissemination
        i. Growth of suitable quantity
        ii. Production facility requirements
        iii. Storage requirements
        iv. Processing requirements
        v. Dispersal requirements
            1. Communicability
            2. Covert dissemination
2. **Likelihood of theft from facility**
    a. Uniqueness of facility as a source for this pathogen
        i. Availability of agent in nature
        ii. Ease of isolating agent from nature
        iii. Availability of agent in other labs
        iv. Availability of agent from biotech pathways
    b. Adversary attributes (threat assessment)
        i. Operational means
        ii. Scientific/technical means
        iii. Opportunity
    c. Facility vulnerabilities (vulnerability assessment)

i. Physical security
    1. Perimeter
    2. Access controls for building with asset
    3. Access controls for room with asset
    4. Access controls to asset
    5. Intrusion detection
    6. Equal treatment of all possible entry points
    7. Alarm assessment
    8. Alarm response

ii. Personnel security
    1. Vetting of unescorted personnel with access to asset
    2. Vetting of unescorted personnel at facility without direct access to asset
    3. Escorting of personnel that have not been vetted
    4. Badges
        a. Use of badges
        b. Access indicators
        c. Identification
        d. Procedures
    5. Training
    6. Employee assistance programs

iii. Transport security
    1. Control of container at facility
    2. Vetting of personnel at facility
    3. Administrative approval process for internal transport
    4. Administrative approval process for external transport
    5. Operational approval process for external transport
    6. Packaging of material for external transport
    7. Selection of external carrier

iv. MC&A
    1. Material presence and identification
    2. Material inventory
    3. MC&A of asset in use
    4. Responsibilities
    5. MC&A procedures

v. Info security
    1. Identification and classification of sensitive information
    2. Protection of sensitive information
    3. Communication of sensitive information
    4. Protection of electronic critical infrastructure
    5. Public disclosure of information

vi. Program management
    1. Roles and responsibilities
    2. Institutional commitment

3. Documentation
4. Exercises
5. Program reviews

3. Consequences of bioattack with the agent

a. Disease consequences (agent properties)
   i. Morbidity
      1. Duration of illness
      2. Severity of illness
      3. Duration of infection
      4. Sequalae
   ii. Mortality

b. Socioeconomic consequences
   i. Economic impact of outbreak of this agent to the country
   ii. Endemicity of this agent in the country
   iii. Active eradication programs of this agent in the country
   iv. Social impact of outbreak of this agent in the country

c. Secondary exposure consequences
   i. Communicability
      1. Human to human transmission
      2. Animal to human transmission
      3. Human to animal transmission
      4. Animal to animal transmission
   ii. Natural routes of infection
      1. Inhalation
      2. Ingestion
      3. Contact
      4. Percutaneous
      5. Vector-borne
      6. Vertical
      7. Sexual
   iii. Survivability in the environment

d. Consequence mitigation measures
   i. Existence of diagnostic tests
   ii. Diagnostic tests available in country for this agent
   iii. Existence of post-exposure treatments
   iv. Post-exposure treatments available in country for this agent
   v. Existence of preventative vaccines
   vi. Vaccines available in country for this agent
   vii. Availability of additional secondary consequence mitigation measures

4. Scalars

a. Adversary motive
b. Adversary technical means

Likelihood agent can be used as a weapon

This section includes factors that were captured as "task complexity" in the previous version of BioRAM.[190]

I. Agent Properties

a. Route of infection

These criteria define the ability of this agent to move from anything, including inanimate objects, into the host (routes of infection). These will be scored based on the agent's ability to be as a weapon. Therefore, for some agents, there will be routes identified in this section that are not considered typical routes of infection.

i. Inhalation

These criteria define the agents ability to cause infection via droplets that have entered the upper or lower respiratory tract.

4 = Preferred route
2 = Possible route
1 = Unknown
0 = Not a route

ii. Ingestion

These criteria define the agent's ability to cause infection via contact with the GI tract

4 = Preferred route
2 = Possible route
1 = Unknown
0 = Not a route

iii. Percutaneous

This criteria defines the agents ability to cause infection through compromised skin

4 = Preferred route
2 = Possible route
1 = Unknown
0 = Not a route

iv. Contact

These criteria define the agent's ability to cause infection through the mucosal membranes.

4 = Preferred route
2 = Possible route
1 = Unknown
0 = Not a route

[190] R. M. Salerno and J. Gaudioso, CRC Laboratory Biosecurity Handbook, 2007.

v. Vector-borne

This criterion defines the agent's ability to cause infection by an animate carrier; this criterion was added to help capture agents that have an increased likelihood of infection if transmitted by a vector than from a percutaneous exposure.

4 = Preferred route
2 = Possible route
1 = Unknown
0 = Not a route

b. Infectious dose

i. Inhalation
4 = Less than 1000 or unknown
0 = Higher than 1000

ii. Ingestion
4 = Less than 1000 or unknown
0 = Higher than 1000

iii. Percutaneous
4 = Less than 1000 or unknown
0 = Higher than 1000

iv. Contact
4 = Less than 1000 or unknown
0 = Higher than 1000

v. Vector-borne
4 = Less than 1000 or unknown
0 = Higher than 1000

c. Stability outside the host

This criterion defines the agent's stability outside the host.

4 = Agent is extremely stable (very resistant to disinfectants), such as prions and bacterial spores
3 = Agent is very stable (high level of resistance to disinfectants), such as Coccidia and *Mycobacterium*
2 = Agent is stable (intermediate level of resistance to disinfectants), such as non-lipid viruses and fungi,
1 = Agent is not very stable outside the host (low level of resistance to disinfectants), such as rickettsiae, chlamydiae, and vegetative bacteria
0 = Agent is fragile outside of the host (very low level of resistance to disinfectants),such as lipid-containing viruses

d. Awareness of Agent's BW potential

This criterion evaluates past BW / BT use of the agent, and any evidence of terrorist interest in this agent.

4 = Agent has a history of use in bioterrorism or biowarfare

2 = Agent has no history of use but there is evidence of terrorist interest
0 = No history of this agent in biowarfare or bioterrorism and no evidence of terrorist interest in this agent

II. Production and Dispersal

a. Growth of suitable quantity

This criterion evaluates the ease (or difficulty) of growing a suitable quantity of the agent.

4 = Suitable quantity of this agent could be produced easily
2 = Production of a suitable quantity of this agent is straightforward for an individual with undergraduate level microbiological skills
1 = Production of a suitable quantity of this agent requires advanced technical skills
0 = Groundbreaking techniques would be required to grow a suitable quantity of this agent

b. Production facility requirements

This criterion evaluates the ease of covertly producing a suitable quantity of this agent.

4 = Production could easily be done covertly
2 = Covert production feasible but some infrastructure required
1 = Production would require sophisticated infrastructure
0 = Facility for producing this agent would be nearly impossible to make covert

c. Storage requirements

This criterion evaluates storage requirements of this agent during production and prior to dissemination. Is it stable (cold storage requirements)?

4 = Agent is stable long-term without cold storage
3 = Agent is stable long term but cold storage required
2 = Agent is stable for days - weeks
0 = Agent is not stable

d. Processing requirements

This criterion evaluates any processing requirements prior to dissemination (e.g. lyophilization, other weaponization requirements).

4 = Agent does not require processing prior to dissemination
3 = Agent can easily be processed into a dry form for dissemination
2 = Processing into a dry form for dissemination is difficult but processing for a liquid dissemination is less challenging
1 = Processing into a form suitable for dissemination requires advanced techniques

0 = Groundbreaking techniques are required to process the agent into a form suitable for dissemination

e. Dispersal requirements
    a. Communicability
        4 = host to host transmission can be used as a dissemination pathway to execute an attack
        0 = host to host transmission cannot be used as a dissemination pathway to execute an attack

    b. Covert dissemination
        4 = Agent can be disseminated both overtly and covertly
        0 = Covert dissemination would be very difficult or nearly impossible

Likelihood of theft from facility

I. Uniqueness of facility as a source for this pathogen
    a. Availability of the agent in nature
        4 = Agent does not exist in nature
        3 = Agent has very limited natural sources
        2 = Agent has limited natural sources
        1 = Agent exists in the environment in the country
        0 = Agent exists in the environment with a global distribution

    b. Ease of isolating agent from nature
        4 = Isolation from nature is not feasible
        3 = Isolation from nature requires advanced technical skills
        1 = Experienced technician required for isolation
        0 = Isolation of viable, virulent agent from nature is trivial

    c. Availability of the agent in other laboratories
        4 = Agent not in other labs in country and is only found in very few labs globally
        3 = Agent rarely found in laboratories within the country
        0 = Agent common in other laboratories within the country

    d. Ease of acquiring agent from other labs
        4 = Agent is highly regulated
        2 = Agent rarely subject to biosecurity regulations anywhere
        1 = Agent not subject to biosecurity regulations in the country
        0 = Agent not subject to biosecurity regulations anywhere

    e. Availability of the agent from biotech pathway
        4 = Synthetic creation requires ground breaking techniques
        2 = Synthetic creation is feasible

0 = Synthetic creation is trivial

II. Adversary attributes (threat assessment)

a. Operational Means

Adversary means to execute theft of agent from the facility; not adversary means to execute BT (see scalars)

4 = Adversary has extensive operational skills and knowledge and all of the necessary tools to execute a theft

2 = Adversary has incomplete operational skills, knowledge, and tools necessary to execute a theft or the adversary means are unknown

0 = Adversary has no means to execute a theft

b. Opportunity

Adversary opportunity to execute theft of agent from the facility. This is simply a binary variable to capture whether the adversary is an insider or outsider. Facilities get credit for limiting the number and extent of insider access under the next section, facility vulnerabilities.

4 = Adversary has authorized access to the facility

0 = Adversary does not have authorized access to the facility

III. Facility vulnerabilities (vulnerability assessment)

a. Physical security

Physical security is a set of countermeasures, designed to reduce the risk of unauthorized access to specific areas or assets. This should involve proactive measures to identify vulnerabilities and implementation of effective control and monitoring mechanisms. This may be accomplished by the concerted effects of fundamental elements such as boundaries, access controls, intrusion detection, alarm assessment and appropriate response and reporting. 4 D: Delay, deny, deter, detect.

i. Perimeter

4 = Facility has no perimeter

3 = Facility has a partial perimeter

0 = Facility has a clearly defined perimeter (natural or man-made)

ii. Access controls for building with asset

4 = Building has no access controls

3 = Building has only procedural access controls

2 = Building has manual access controls

1 = Building has electronic access controls based on something person has (e.g. swipe card)

0 = Building has electronic access controls tied to person, e.g. knowledge (e.g. PIN) or biometrics

iii. Access controls for room with asset (lab, storage area)
4 = Room has no access controls
3 = Room has only procedural access controls
2 = Room has manual access controls
1 = Room has electronic access controls based on something person has (e.g. swipe card)
0 = Room has electronic access controls tied to person, e.g. knowledge (e.g. PIN) or biometrics

iv. Access controls to asset (pathogen isolates, repository stocks)
4 = Asset has no access controls
3 = Asset has only procedural access controls
2 = Asset has manual access controls
1 = Asset has electronic access controls based on something person has (e.g. swipe card)
0 = Asset has electronic access controls tied to person, e.g. knowledge (e.g. PIN) or biometrics

v. Intrusion detection
4 = No intrusion detection
3 = Only detection is staff trained to report anything unusual
2 = Detection based on observations by personnel, including roving guard patrols
1 = Local annunciation of alarms only
0 = Alarms for intrusion detection are reported to a central alarm station

vi. Equal treatment of all possible entry points
4 = No controls (access controls and/or intrusion detection) on any entry points
1= Controls only on doors
0 = Controls on all possible entry paths through barrier (e.g. glass break sensors on windows)

vii. Alarm assessment
4 = No alarm assessment
3= Only alarm assessment is staff trained to report
2= Guards sent to assess alarms
1 = Alarm assessed by camera
0 = Alarm assessed by camera that records brief time before alarm and then afterwards

viii. Alarm response
4 = No plans for alarm response
2= Local law enforcement is initial response and a MOU is in place for this
1 = Local law enforcement is initial response, MOU in place, and this is exercised regularly OR Onsite guard response
0 = Onsite guard response and LLE back-up with MOU and regular exercises

b. Personnel security

Personnel security is designed to ensure that only trustworthy individuals are authorized to access restricted areas or assets. The level of screening and required standards, should be commensurate with the deemed position risk. Personal security is the primary barrier for addressing the insider threat.

i. Vetting of unescorted personnel with access to asset
4 = No vetting of personnel prior to granting access
3 = Vetting includes only verification of credentials (education, prior employment) and references
2 = Vetting includes verification of credentials, references, and criminal history
1 = Vetting includes verification of credentials, references, criminal history, and additional checks for derogatory information (e.g. financial checks, drug screening, interviews of contacts, personality tests)
0 = Vetting includes all of above and regular reevaluation intervals are established

ii. Vetting of unescorted personnel at facility without direct access to asset
4 = No vetting of personnel prior to facility access
3 = Vetting includes only verification of credentials (education, prior employment) and references
2 = Vetting includes verification of credentials, references, and criminal history
1 = Vetting includes verification of credentials, references, criminal history, and additional checks for derogatory information (e.g. financial checks, drug screening, interviews of contacts, personality tests)
0 = Vetting includes all of above and regular reevaluation intervals are established

Note: #1 and #2 can be applied multiple times if different types of people with access to the facility are screened differently (e.g. scientist vs technician vs animal care worker vs housekeeping vs guards, etc)

iii. Escorting of personnel that have not been vetted (including visitors, maintenance or other contract personnel)
4 = Allowed unescorted access to room with asset
3 = Administrative escorting to room with asset allowed
2 = Escorting requirements in place but not defined escort ratios
1 = Escort ratios defined
0 = Escort ratios defined, dates/times of escorted visitors recorded

iv. Badges
a. Use of badges
4 = Not required or routinely worn
0 = Badges required
b. Access indicators
4 = No indicators of who has access where
0 = Badges indicate level of access
c. Identification
4 = No way to identify if badge belongs to person wearing it
0 = Badges have a photo and expiration date
d. Procedures
4 = No badge procedures
0 = Procedures are in place for lost badges and turning in badges when access in no longer needed

v. Training
4 = No biosecurity training provided
2 = Biosecurity training provided to anyone with unescorted access
1 = Biosecurity training provided to all employees
0 = Biosecurity training provided to all employees and on-site contractors (e.g. guards)

vi. Employee assistance programs
4 = No support systems in place
3 = Informal support network among personnel
2 = Formal employee assistance program in place
1 = And employees not penalized if access voluntarily suspended due to a temporary situation
0 = And anonymous whistleblower / omsbuds mechanism in place

c. Transport security

Transport security covers both the threat from insiders and outsiders, by implementing materials control and accountability mechanisms to reduce the risk of theft, inappropriate handling and misplacement while material is being transported between restricted and appropriate pre-approved areas.

1. Control of container at facility (internal transport including shipping/receiving areas)
   4 = No controls during internal transport
   3 = Agent transported by authorized individual but may be left unattended in unsecured areas
   1 = Agent not left outside of custody of authorized individual during transit unless secured but level of security is lower than how it is secured in storage
   0 = Agent not left outside of custody of authorized individual during transit unless secured in a manner equivalent or better to how it is secured in storage

2. Vetting of personnel at facility (internal transport including shipping/receiving areas)
   4 = Facility personnel who have access to materials during internal transport are not vetted
   2 = Facility personnel who have access to the materials during internal transport are vetted but to a lower degree than those who handle the agent in the laboratory
   0 = Facility personnel who have access to materials during internal transport are vetted to the same degree or better as personnel who handle the agent in the laboratory

3. Administrative approval process for internal transport (MC&A)
   4 = No approvals or documentation required for internal transport
   2 = Pre-approval not required for internal transport but transfer is documented in laboratory records
   0 = Pre-approval required for internal transport and the transfer is documented in laboratory records

4. Administrative approval process for external transport
   4 = No approvals or documentation required for external transport
   3 = Pre-approval not required for external transport but transfer is documented in laboratory records
   1 = Pre-approval by a responsible individual at the facility required prior to shipping to external recipient

0 = And a material transfer agreement is required prior to final approval or an external regulatory body must approve the transfer prior to shipment

5. Operational approval process for external transport
   4 = No biosecurity (or biosecurity status is unknown) at receiving facility
   2 = Receiving facility has biosecurity but their level of security is lower than at shipping facility
   1 = Receiving facility has equivalent or better biosecurity
   0 = And notifications between shipping and receiving facility at time of dispatch and receipt, respectively

6. Packaging of materials for external transport
   4 = Agent can be identified by examining labels on outside of the package
   0 = Conforms to infectious substance shipping labeling requirements but does not identify the specific agent on the outside of the package. Packaging should not attract any special attention/anonymous labeling. (Lost-in-the-crowd).

7. Selection of external carrier
   4 = No thought is given to security in selection of carrier
   2 = External carrier chosen that has good reputation for security of commercial shipments (e.g. FedEx, DHL, Airborne Express)
   0 = And the carrier has a security plan in place that covers shipments of dangerous biological agents

d. Material Control & Accountability

MC&A security involves establishing and reinforcing responsible oversight mechanisms, when working with or storing dangerous pathogens and toxins. The objective is to establish procedures that discourage primarily insiders from obtaining and using biological materials offensively. MC&A will help in not only deterrence, but possibly also in detecting theft, and facilitates forensic analysis in case of illicit diversion.

i. Material – presence and identification
   4 = No materials are subject to MC& measures
   3 = Individual PIs/lab owners make decisions about which materials require MC&A measures
   2 = Facility just relies on regulatory or international lists (e.g Select agent list, Australia Group list) to determine which materials at their facility need MC&A measures

1 = Facility risk assessment to identify and categorize those materials and forms of materials that require MC&A measures

0 = And, where applicable, proactive measures towards the reduction of risk through elimination, substitution or minimization of volumes/quantities of agents, and the type and number of manipulations conducted.

ii. Material inventory

4 = No material cataloging

3 = Seed stock inventory electronically managed

2 = Seed stock inventory actively managed and working stocks, including infected animal status, tracked through laboratory notes

1 = Seed stock inventory electronically managed using a secure system and includes tracking of samples that have been transferred into and out of the lab, source, strain, controlled substance identification, form, responsible individual, etc.

0 = Seed and working stock containers bar coded or otherwise identified, marked and cataloged for inventory tracking purposes.

iii. Material control of asset in use (working stocks, infected animals, etc)

4 = No controls in place when materials are in use

2 = Controls in place when materials are in use (e.g. working tissue cultures, animals subjected to challenge experiments, in equipment such as incubators and centrifuges, etc.) but at lower level than controls for material in storage

0 = Controls in place when materials are in use (e.g. working tissue cultures, animals subjected to challenge experiments, in equipment such as incubators and centrifuges, etc.) at equivalent level to controls for material in storage

iv. Material accountability responsibilities

4 = No designation of responsibilities

2 = PI aware of each agent used within their laboratory

1 = A responsible individual is designated to oversee the control of protected agents

0 = A qualified and vetted individual is designated to oversee the control of protected agents (agent-by-agent basis, on a per-laboratory basis, etc.)

v. Material accountability procedures

4 = No procedures for MC&A exist

2 = Some MC&A procedures are in place but they are not comprehensive and/or are not fully implemented
0 = Written procedures are in place and implemented to ensure timely and accurate recording, reporting and auditing of materials subject to MC&A measures

e. Information security

Information security is a set of tools and practices used to protect sensitive information.

i. Identification and classification
4 = No identification and classification of information in place
1 = Sensitive (security-related) information is identified, marked, and classified at a level equivalent to the risk

ii. Protection
4 = No protection of information
2 = Some information protection procedures are in place but they are not comprehensive and/or are not fully implemented
0 = Protecting sensitive (security-related) information at a level equivalent to the risk (e.g. information considered a valuable asset is held redundantly by the institution. Information is accessed on a need-to-know basis, by pre-approved/screened authorized individuals. Procedures for handling, storing, transmitting, and destroying sensitive information)

iii. Communication of sensitive information
4 = No communication policies
2 = Staff is trained on communication policies
0 = Means of communicating sensitive information is controlled (e.g. encryption for electronic transmission, no cellular discussions or communication/viewing sensitive materials).

iv. Protection of electronic critical infrastructure

Electronic critical infrastructure includes inventory databases, alarm control stations, access control systems, building monitoring systems, etc

4 = No protection (e.g. adversary can access the systems through the internet)
2 = Basic good practices are in place (e.g. firewalls, desktop security)
0 = Comprehensive IT security infrastructure in place or not applicable because no sensitive information is stored

v. Public disclosure of information
4 = No public disclosure procedures/policies in place

2 = Some procedures/policies regarding public disclosure are in place but they are not comprehensive and/or are not fully implemented
0 = Potentially sensitive (security-related) information is screened prior to public release, by an established review and approval process. Modification of information to make it appropriate for public release

f. Program Management

Program Management guides and oversees the implementation of the biosecurity program. The organization should establish, document, implement and maintain a program management system in accordance with legal requirements, and/or stated objectives.

i. Roles and responsibilities
4 = No identification of or education on roles and responsibilities
3 = Facility personnel are educated on their biosecurity responsibilities
2 = Biosecurity officer is identified
0 = Management ensures roles, responsibilities and authorities are defined, documented and communicated

ii. Institutional commitment
4 = Management at facility is not aware or interested in biosecurity concerns
3 = Management at facility is aware of biosecurity concerns but has not implemented a biosecurity policy or devoted resources to address the issue
2 = Management has made some efforts to improve biosecurity at the facility but they are not comprehensive and/or are not fully implemented
1 = Facility has a comprehensive biosecurity policy, developed, authorized and signed by top management. The policy shall be appropriate to the nature and scale of the risk. Management establishes the commitment and objectives of the biosecurity system, and communicates this to all stakeholders.
0 = Management identifies and prioritizes program needs and allocate funds as necessary

iii. Documentation
4 = Facility has no biosafety or biosecurity policies, manuals, or SOPs
3 = Facility has biosafety policies, manuals, or SOPs but no specific biosecurity documentation

2 = Facility has some biosecurity documentation but they are not comprehensive and / or not fully implemented
1 = Facility has biosecurity policies, manuals, and SOPs
0 = Facility's biosecurity documentation also includes risk assessment and incident response information

iv. Exercises
4 = Facility does not conduct any biosecurity exercises
2 = Facility conducts tabletops or other exercises on an ad hoc basis
1 = Facility conducts annual exercises
0 = Facility includes external responders in their exercises

v. Program reviews
4 = No review of biosecurity program conducted
3 = Biosecurity program is reviewed and revised as necessary after any incidents or near-incidents
1 = Biosecurity program is subject to internal self-assessments
0 = Management ensures continual improvement, conducts routine self-assessments, and ensures actions taken are corrective and preventive in nature. Reviews include assessing opportunities for improvement and need for changes to the system, procedures, policies and objectives.

Consequences of bioattack with agent

Agent disease properties, socioeconomic consequences, secondary exposure consequences, and mitigation measures. Consequence is defined by the extent of disease and those factors which may be used to mitigate the consequence for a specific host population and normalized to that population.

I. Disease consequences (agent properties)

a. Morbidity

Morbidity is the severity of illness that the pathogen creates in the host. Severity is measured by these sub-criteria.

i. Duration of illness

This criterion is scored based on the average length of time of clinical signs of infection in a healthy host.
4 = long duration (months or more)
3 = moderate duration (week(s))
1 = short duration (days)
0 = No signs of infection

ii. Severity of illness

This criterion will be scored based on the average severity of illness, ranging from no signs of illness to hospitalized in critical condition.

4 = Extreme sign of disease (ICU)
3 = High sign of disease (not able to function (hospitalized))
2 = Moderate sign of disease (able to function in a limited manner (bed rest))
1 = Low sign of disease (able to function but showing symptoms)
0 = No sign of disease

iii. Duration of infection (chronicity)

This criterion measures the length of time the host is infected with the organism

4 = Infection present for life of host
3 = Infection present post clinical signs for months
2 = Infection present post clinical signs for weeks
1 = Infection present if clinical signs
0 = No sign of disease

iv. Sequelae

This criterion measures the conditions resulting from an infection of this agent

4 = High long-term impact which renders the host unable to function normally
2 = Moderate long-term impact which hinders the hosts ability to function normally
1 = Mild long-term impacts do not impede the hosts ability to function normally
0 = No long term impact

b. Mortality

A measure of the frequency of death caused by the pathogen in a defined population during a specified interval of time. This is measured by expected unvaccinated and untreated frequency of death.

4 = High mortality (75% or more)
2 = Medium mortality (15% to 74%)
1 = Low mortality (1% to 14%)
0 = No Mortality (0%)

c. Disease impact on the population

Consider herd immunity/levels of vaccination, immunocompromised population, etc

4 = Impacts a diverse population, including healthy adults
2 = Impacts only segments of the population (e.g. elderly, children, immunocompromised)

0 = No expected population impact

II. Socioeconomic consequences

This assessment is an order of magnitude assessment based on expert judgment

a. Economic impact of outbreak of this agent to the country

This is the economic impact as related to the agent infecting humans. Animal impacts are assessed separately. Animals: National economic impact, farm costs, loss of breeding stock, future earnings, regional economic impacts…

4 = The economic impact of an agent release from the facility would be catastrophic

2 = The economic impact of an agent release from the facility would be moderate

0 = The economic impact of an agent release from the facility would be negligible

b. Endemicity of this agent in the country

This criterion will score how endemic the agent is within the country.

4 = The agent is absent in the environment of the country

3 = The agent is not endemic in the country, but outbreaks may occur

0 = The agent is endemic in the country

c. Active eradication programs of this agent in the country

For agents with active eradication program, there may be additional requirements.

4 = The country is in the process of eradicating this agent

0 = The country does not have an active eradication program for this agent

d. Social impact of outbreak of this agent in the country

For malicious release: public panic, rioting, – People being unwilling to go out and work, fear of additional agents or of more incidents – multiple incidents

4 = The social impact of an agent release from the facility would be catastrophic

2 = The social impact of an agent release from the facility would be moderate

0 = The social impact of an agent release from the facility would be negligible

III. Secondary Exposure Consequences

a. Communicability

Host to host transmission

i. Human to human

0 = No human to human transmission

2 = Unknown
4 = Human to human transmission

ii. Animal to human
0 = No animal to human transmission
2 = Unknown
3 = Single species transmission to humans
4 = Transmission from multiple species to humans

iii. Human to animal
0 = No human to animal transmission
2 = Unknown
4 = Human to animal transmission

iv. Animal to animal
0 = No animal to animal transmission
2 = Unknown
3 = One species only
4 = Transmission between multiple species

b. Natural routes of infection

These will be defined as they were for laboratory routes of infection, but the scores will reflect the natural routes of infection and included routes which are not seen in a laboratory.

i. Inhalation
These criteria define the agents ability to cause infection via droplets that have entered the upper or lower respiratory tract.
4 = preferred route
2 = possible route
1 = unknown
0 = not a route

ii. Ingestion
These criteria define the agent's ability to cause infection via contact with the GI tract
4 = preferred route
2 = possible route
1 = unknown
0 = not a route

iii. Contact
These criteria define the agent's ability to cause infection through the mucosal membranes.
4 = preferred route
2 = possible route

1 = unknown
0 = not a route

iv. Percutaneous

This criteria defines the agents ability to cause infection through compromised skin

4 = preferred route
2 = possible route
1 = unknown
0 = not a route

v. Vector-borne

This criterion defines the agent's ability to cause infection by an animate carrier; this criterion was added to help capture agents that have an increased likelihood of infection if transmitted by a vector than from percutaneous exposure.

4 = preferred route
2 = possible route
1 = unknown
0 = not a route

vi. Vertical

This criterion defines the agent's ability to cause infection by an animate carrier; this criterion was added to help capture agents that have an increased likelihood of infection if transmitted by a vector that from percutaneous exposure.

4 = preferred route
2 = possible route
1 = unknown
0 = not a route

vii. Sexual

This criterion defines the agent's ability to cause infection by an animate carrier; this criterion was added to help capture agents that have an increased likelihood of infection if transmitted by a vector than from percutaneous exposure.

4 = preferred route
2 = possible route
1 = unknown
0 = not a route

c. Survivability in the environment

This criterion defines the agent's stability in the environment; this includes soil, water, fecal matter, etc. Resistance to disinfection is used as a marker for stability.

4 = Agent is extremely stable (very resistant to disinfectants), such as prions and bacterial spores
3 = Agent is very stable (high level of resistance to disinfectants), such as Coccidia and *Mycobacterium*
2 = Agent is stable (intermediate level of resistance to disinfectants), such as non-lipid viruses and fungi,
1 = Agent is not very stable outside the host (low level of resistance to disinfectants), such as rickettsiae, chlamydiae, and vegetative bacteria
0 = Agent is fragile outside of the host (very low level of resistance to disinfectants),such as lipid-containing viruses

IV. Consequence Mitigation measures

a. Existence of diagnostic tests
0 = No
2 = Unknown
4 = Yes

b. Existence of post exposure treatments (including immuno-globulin, vaccines and anti-microbials
0 = None
2 = Partially effective
4 = Effective

c. Existence of preventative measures (vaccines)
0 = No vaccine
2 = Partially effective (will not prevent but will limit the impact of the disease – only effective in a small population)
4 = Effective

d. Diagnostic tests for this agent available in country
The effectiveness in general of diagnostic tests has been defined elsewhere; this is the criterion to measure the ability to use these diagnostic tests in the country.
4 = Diagnostic tests are not available in the region for this agent
0 = Diagnostic tests are available in the region for this agent

e. Post-exposure treatments available in country of this agent
The effectiveness in general of post-exposure treatments has been defined elsewhere; this is the criterion to measure the ability to use these treatments in the country.
4 = Treatments are not available in the region for this agent
0 = Treatments are available in the region for this agent

f. Vaccines available in the region for this agent

The effectiveness of vaccines has been defined elsewhere; this is the criterion that measures the ability to use these vaccines at local health service institutions.

4 = Vaccines are not available in the region for this agent
0 = Vaccines are available in the region for this agent

g. Availability of additional secondary consequence mitigation measures
   4 = Isolation / quarantine / culling of impacted population is not feasible
   0 = Isolation / quarantine / culling of impacted population is doable

Scalars

Scalars modulate the overall risk

a. Adversary motive
   4 = Adversary intends to conduct a large-scale bioterrorism event, causing mass murder, mass hysteria, or devastating economic impact
   3 = Adversary seeks to conduct a small-scale bioterrorism incident
   2 = Adversary is interested in making a political statement
   1 = Theft would be for personal gain (e.g., economic or revenge; i.e. a biocrime)
   0 = Adversary has no interest in biological agents

b. Adversary technical means
   4 = Adversary has the necessary skills and equipment to achieve their motive
   2 = Adversary has some of the necessary skills and equipment to achieve their motive
   0 = Adversary lacks the necessary skills and equipment to achieve their motive

APPENDIX D – FIRST SURVEY SUMMARY OF RESPONSES

Respondents: Morocco (1), India (5), Argentina (1), Uganda (2), Vietnam (1), Philippines (4), Kenya (2), Taiwan (2, Pakistan (1), Sri Lanka (1), China (1), Malaysia (1), Mexico (1), Thailand (1)

Does your institution perform formal, documented biosafety and/or biosecurity risk assessments? If so, who conducts the assessments? Briefly describe your methodology:

Some (10) not doing any assessments. Others mostly rely on biosafety officer or biosafety committee. A few make the PI responsible for the risk assessments. No one described an actual methodology.

Who decides what are appropriate biosafety and/or biosecurity measures, (ie who decides what risks are acceptable or unacceptable)? Are community perspectives considered in these decisions?

Responses split between scientists, BSOs, IBCs, and occasionally the director. Only a handful of respondents consider community perspectives.

Do you evaluate the effectiveness of your biosafety and biosecurity programs? If so, how often do you do a formal evaluation? What metrics do you use? Do you use a management system at your institution? If so, which one?

Only a few look at how effective their programs are; none had established metrics for this review but many were interested.

A few labs used ISO (9001, 15189:2003, 17025).

Does your institute address biosafety and biosecurity in an integrated manner or separately? What are the biggest challenges for you to implementing biosafety and biosecurity in an integrated system?

Separately: 13
Integrated or moving towards an integrated system: 11

Challenges: lack of awareness, resources, lack of explicit policies/regulation, lack of management support

Are you aware of the CEN Biorisk Management standard? If so, are you considering implementing it at your facility? Why or why not? Would you be interested in being certified to the CEN Standard? Why or why not?

Aware - Yes: 14
Aware - No: 10
Most are interested in implementing it even if they have not heard of it because: Want to meet international standards, Expect the standard will help them improve their situation, View it as a good learning opportunity

APPENDIX E – SECOND SURVEY SUMMARY OF RESPONSES

Definitions

(adapted from CWA 15793:2008 Laboratory Biorisk Management Standard and the U.S. National Safety Council)

Biological agent: any microorganism including those which have been genetically modified, cell cultures and endoparasites, which may be able to provoke any infection, allergy or toxicity in humans, animals or plants

Biosafety: laboratory biosafety describes the containment principles, technologies and practices that are implemented to prevent the unintentional exposure to biological agents and toxins, or their accidental release

Biosecurity: laboratory biosecurity describes the protection, control and accountability for biological agents and toxins within laboratories, in order to prevent their loss, theft, misuse, diversion of, unauthorized access or intentional unauthorized release

Incident: An incident is an unplanned, undesired event that adversely affects completion of a task (in conducting research with biological agents and toxins) or causes harm.

Serious incident: An incident that results in exposure, accidental release, loss, theft, misuse, diversion of, or intentional unauthorized release of biological agents or toxins

Near miss: An incident that does not result in exposure, release, or loss of biological agents or toxins

---

1. From your institution's perspective, what are the main drivers or reasons for implementing biorisk policies and management systems? Please rank the importance of these drivers for your institution separately from a biosafety and a biosecurity perspective (1 is the most important to your institution and the highest number (e.g. 17) is the least important driver). Please include any other drivers that are important for your institution:

	Biosafety	Biosecurity
	Values are averages	
To comply with rules and regulations	**2.2**	**2.7**
To comply with guidance documents	**4.4**	**5.1**

To meet internally accepted best practices	**5.4**	**5.6**
To meet external industry standards	**8.0**	**8.9**
To reduce the risk of economic	**9.3**	**8.6**
To attract, maintain, or increase research funding	**9.5**	**9.3**
To foster innovation	**11.7**	**12.1**
To reduce the risk of theft of materials or intellectual property	**8.4**	**3.5**
To protect the community, environment, and workers	**2.4**	**2.9**
To satisfy public demand for transparency or ethical behavior	**6.8**	**7.5**
To reduce the risk of a tarnished institutional image	**7.0**	**7.0**
To build a safety and/or security culture	**4.9**	**5.5**
To heighten personnel morale	**8.0**	**9.3**
To ensure business continuity	**7.8**	**7.8**

2. Do you agree with the incident definitions on the first page?
   a. Incident: **17 agreed, 6 did not**
      a. If no, why not?
         One cited the definition in CWA 15793. Several were concerned with the term "harm" and the second part of the statement, preferring a more thorough and precise definition. Another preferred broader definitions. Another would divide incidents into events in which harm could have occurred and events into which harm did occur. One person also emphasized OHSAS 18001:2007.

      b. Serious incident: **16 agreed, 7 did not**
         a. If no, why not?
            One cited the definition in CWA 15793. Others believed the definition should specify "serious harm" or "exposure leading to serious injury or fatality" as well as preferred the use of the term "accident" instead of "incident" and thus conform to

OHSAS 18001:2007. Another thought the definition should be broader and include incidents not necessarily related to biorisk.

c. Near miss **16 agreed, 7 did not**

a. If no, why not?

One cited the definition in CWA 15793. Others believed the definition needed to be broader to include incidents unrelated to biorisks. Others thought the definition should specify that near misses <u>almost</u> or at least had the potential to result in adverse effects. Others would have liked emphasis on "exposure." Another thought a release which did not result in exposure to be considered a near-miss. One was worried the term "near-miss" was not very scientific.

3. Do you use a system/process for reporting incidents (as defined above)? **13 said Yes, 10 said No**

a. If yes, please describe:

One responded that investigation requirements varied according to the nature of the incident. Several described forms that must be filled out after an incident. Others described electronic forms and databases and follow up from EHS. One said the system was in place only for biosafety incidents, and other specified that reports were formulated specifically to inform superiors. One described requirements to report to regulatory bodies outside of the organization. Another described their reporting system as very strict and requiring a report for any sort of incident. Another said the person who witnessed the incident had the responsibility to fill out a form. One said the process was just a written or verbal communication to inform their superiors. Another said there were strict legal guidelines to report any incidents internally as well as externally to officials in government.

b. If yes, do you also have a system for investigating those incidents?

Of the 13 that said yes, 9 said yes to this question also. One said they used the submitted forms to establish the cause of the incidents.

4. Do you use a system for reporting serious incidents (as defined above)? **12 said Yes, 11 said No**

a. If yes, please describe:

Most of the responses, including one NO response, mentioned their institution did not have a system in place any different for serious incidents than for regular incidents or other deviations from "normal". One person specified a system similar to that described by others for incidents, but in his institution, it is only employed for "serious incidents". One person said they had no system other than the responsibility of the person in charge of

the laboratory to inform the administration. One said all incidents were reported and the rating was done during investigation and analysis. One said a written or verbal communication just to inform their superiors.

b. If yes, do you also have a system for investigating those serious incidents?
Of the 12 that said YES to question 4a, 6 said YES to 4b. One said that seriousness of incidents was reviewed in a monthly meeting which reviewed all incidents.

5. Do you use a system for distinguishing serious incidents from near-misses (as defined above)? **5 said YES, 18 said NO**
   a. If yes, please describe:
   Of those who responded YES, one said that there was a field in their normal incident form that asked whether the incident was a near-miss or if it was serious. One specified that different forms were filled out for near misses and serious incidents. Another mentioned that when there was an incident, an internal assessment involving a senior technical, scientific, medical and lab safety officer occurred to determine the seriousness of the event. One said usually the incident was not reported if there was no harm inflicted.

   b. If yes, do you also have a system for investigating near misses?
   Of the 5 that said YES to question 5a, 3 said YES to question 5b.

6. If you use a reporting and investigation mechanism for incidents (either serious incidents or near misses), where do you use the lessons-learned from these reports/investigations to improve the biosafety and biosecurity (mark all that apply)?
   a. No reporting or investigation
   2 said Yes
   b. Only within the specific lab or facility where the incident occurred**7**
   7 said Yes
   c. Throughout the institution
   14 said Yes
   d. We share our lessons-learned with colleagues outside our institution
   6 said Yes
   e. Other (please describe):
   5 said Yes
   One person said only on health and safety issues throughout their institution. Another said their lab shared their lessons learned with another lab in their institution. Another said

information was kept as a report shared only to senior management, and never actually discussed openly. One person reported that there had been occasions that news was released to the media – information was bought by "media people" from some of the lower rank employees. One said they used lessons learned during an EHS forum and other meetings and conferences. Another said they had a person which handled the electronic reporting system which also made sure that safety events / incidents in one division were discussed in safety meetings in other divisions; the person also responsible for safety audits and follow up on corrective actions.

7. Do you think it would be helpful to managing biosafety and biosecurity at your institution to learn about incident (either serious incidents or near misses) investigations and lessons-learned from other institutions around the world? **21 out of 23 respondents said yes**
    a. If yes, why do you think it would be helpful?
    There was a general appreciation for the ability of sharing information and lessons between institutions to increase safety and security in laboratories. One said the issue was mostly discussed with EBJA. Another said increasing awareness of what can go wrong and reviewing one's own processes and procedures accordingly – could be used to demonstrated to end-users as part of influencing behavior. One was interested in learning about investigations and lessons learned in similar institutions, becoming aware of circumstances, in order to try to prevent incidents. Another was interested in using other labs as references or models for their own lab. One thought knowing the experience of others was always interesting and helpful to be aware of. Prevention of similar incidents in particular was highlighted by another. One said it was useful in order to provide evidence that incidents may happen in labs.

    b. If no, why do you think it would NOT be helpful?
    Of the 2 that did not say yes, one did not respond and the other said it was "not relevant" but explained no further.

8. Does your facility have a written biosecurity or general security plan? **15 said Yes, 8 said No. One said their plan was being drafted.**

Does this plan include response actions? **15 said Yes, 8 said No**

Does it identify who outside of your facility you need to contact for support (like local law enforcement)? **13 said Yes, 10 said No**

9. Does your facility have a written biosafety or general safety plan? **17 said Yes, 6 said No**

Does this plan include response actions? **15 said Yes, 8 said No**

Does it identify who outside of your facility you need to contact for support (like emergency responders)? **15 said Yes, 8 said No**

10. Do you train or exercise on these plans?
    - **a.** Yes, both biosafety and biosecurity plans **6 said Yes**
    - **b.** Yes, biosafety plan only **7 said Yes**
    - **c.** Yes, biosecurity plan only **1 said Yes**
    - **d.** No, neither **4 said Yes**
    - e. If yes, please describe: **4 said YES One said they taught the theory of biosafety and biosecurity for students in the microbiology theme. Another said YES, during annual emergency exercises.**

APPENDIX F – TRAINING COURSE ON TESTING SYSTEM EFFECTIVENESS

As highlighted in the body of this report, testing facility biorisk management plans is a key component of monitoring and improving the effectiveness of an institutions biorisk governance. Under this project, we developed a four hour course on the principles involved in exercising facility biosecurity plans. This was taught as a pre-conference course at the 52nd Annual Biological Safety Conference[191] in Miami, Florida on October 18, 2009. A description of the course and the course agenda are given below; the course materials can be found at www.biosecurity.sandia.gov.

Course Description:
Institutions should document their laboratory biosecurity in a written plan that is designed according to a site-specific risk assessment. *Biosafety in Microbiological and Biomedical Laboratories* recommends that institutes exercise their written biosecurity plans, and the Select Agent regulations require Select Agent labs to test their biosecurity plans at least annually through drills or exercises. This course will review strategies for exercising facility biosecurity plans through tabletop exercises and drills. Course participants will learn how to develop a tabletop exercise that addresses the roles and responsibilities of those involved in biosecurity, and that will help identify any significant deficiencies in their current biosecurity plan. Participants will also share lessons learned. This course will include lecture and facilitated class discussions.

Learning Objectives:

1. Understand the range of adverse events that should be considered in biosecurity plans
2. Understand approaches for exercising biosecurity plans
3. Develop strategies for coordinating with emergency responders to prepare security response plans

[191] http://absaconference.org/

Schedule:

(Students will have a 15 min break approximately 2 hours into course)

- Introduction and discussion
- Design Basis Threat (DBT) and the Role of Risk Assessment
    - What aspects of the RA and DBT need to be incorporated in the security plan
    - Guided discussion on drafting a DBT
- What goes into a security plan
    - Guided discussion on security plan topics
    - Small group activity to outline security a security plan based on the topics defined in the class
- How to exercise the security plan
    - Awareness Training
        - What are the objectives of awareness training
        - When is it the best option
        - Key Considerations
    - Table Tops
        - What are the objectives of a table top
        - When is it the best option
        - Key considerations
    - Full Scale Exercises
        - Objectives
        - When is it the best option
        - Key considerations
- After Action Reports
- Concluding discussion on benefits and challenges to exercising security plans

APPENDIX G – ANNOTATED BIORISK BIBLIOGRAPHY

This annotated bibliography is meant to give readers an introduction to key resources for biorisk management; it is not intended to be comprehensive. It summarizes resources from disciplines predominately outside of the biosafety literature that the authors of this report found to be useful in considering new approaches and thinking for managing biorisks.

Biorisk Cases

1. Summary Report on State, Local, Private, and Commercial Laboratories' Compliance with Select Agent Regulations (January 2008). United States Department of Health and Human Services Office of Inspector General, A-04-06-01033.

The final report summarizes the results of the DHHS Inspector General's reviews of eight state, local, private, and commercial laboratories' compliance with select agent regulations during various periods from November 2003 to September 2005. The individual reports found that, as required, each of the eight entities had appointed a "Responsible Official" to provide management oversight of its select agent program. However, certain other controls at all eight entities did not comply with Federal regulations. Each entity had weaknesses in at least one control area that could have compromised the ability to safeguard
select agents from accidental or intentional loss. The control areas included select agent accountability (i.e. inventory control), restricting access, security plans, training, and incident response plans.

2. Texas A&M University, Report on Site Visit (August 2007). United States Department of Health and Human Services, Centers for Disease Control and Prevention.

The report summarizes the findings of a comprehensive review of a select agent and toxin activities at TAMU conducted by the CDC in July 2007. The observations included failures by the Responsible Official to comply with various aspects of the regulations, incomplete biosafety, biosecurity and incident response plans, missing training documentation, insufficient site-specific operating procedures, and incomplete personnel records related to access and medical monitoring. The suspension of all select agent and toxin activities at TAMU was to remain in effect until all programmatic issues identified by the CDC review had been addressed.

3. Biosecurity in UK Research Laboratories (June 2008). United Kingdom Parliament, Innovation, Universities, Science, and Skills Committee, No. 59A (07-08).

The Committee's report points out that some high containment facilities in the UK are world class but others, such as the Institute for Animal Health at Pirbright and the Health Protection Agency at Porton Down, are in need of significant investment. The summary of the findings included shortcomings in funding for ongoing maintenance and a lack of coordination between organizations that sponsor research requiring high containment laboratories and those that run the facilities.

4. Winnipeg researcher charged with smuggling Ebola material into U.S. (May 2009). http://www.cbc.ca/health/story/2009/05/13/border-biological-agents.html

This article provides an account of a researcher attempting to transport 22 vials of non-infectious genetic material from the Ebola virus across the U.S.-Canadian border. The researcher was previously employed with the Public Health Agency of Canada (PHAC) in Winnipeg but was en route to his new place of employment with the National Institutes of Health in Bethesda, MD. The material did not pose a risk to the public; however, PHAC was evaluating its biosecurity protocols as a result of the incident.

5. Barry, M. A. (March 2005). Report of Pneumonic Tularemia in Three Boston University Researchers. Boston Public Health Commission, Communicable Disease Control.

This report gives a comprehensive overview of the 2004 tularemia outbreak at Boston University. The issues contained in this report highlight the need for additional Citywide safety measures to prevent the recurrence of such an event. The growth in the number of laboratories in the City working with potentially hazardous organisms and substances, including the increase in the amount of research involving Select Agents, requires new and expanded governmental oversight at multiple levels.

Discussion about how best to achieve the proper level of monitoring and oversight must involve officials at the local, state and federal level. However, even while such discussions are proceeding, BPHC believes that positive action steps should be undertaken at a local level to insure the health and safety of microbiology research laboratory workers and the greater Boston community.

6. Palk, J.M. (June 2009). USAMRIID finds 9,200 disease samples it didn't know it had. *Frederick News Post.*

This newspaper article highlights an oversight by the U.S. Army Research Institute of Infectious Diseases uncovered by a full inventory conducted of the Institute's inventory of infectious disease samples in early 2009 that resulted in identifying 9,200 previously unrecorded samples.

7. Miller, J.D. (June 2004). US lab is sent live anthrax. *News for the Scientist*, 5(1):20040611-03 (accessed http://www.the-scientist.com/news/20040611/03/).

This article provides an account of the incident that occurred in the summer of 2004 where a west coast research laboratory was live *Bacillus anthracis* originally thought to be inactivated. The bacteria had been previously tested by laboratory that provided the material as well as when it was received at the Oakland-based facility. Research activities involving mice revealed the bacterial to be alive, resulting in potential exposures to seven laboratory workers. The incident promulgated the laboratories involved, federal authorities, and facilities across the U.S. to evaluate their inactivation and attenuation protocols.

8. Miller, J. (May 2004). Russian Scientist Dies in Ebola Accident at Former Weapons Lab. *New York Times*. http://www.nytimes.com/2004/05/25/international/europe/25ebol.html

This newspaper article provides details of the incident in a Russian laboratory involving the exposure (via needlestick) of a researcher to the Ebola virus working on a vaccine that resulted in her death. While the incident highlights the risks and hazards associated with working in high containment facilities, it also raises concerns about the timeliness of reporting such incidents to appropriate authorities. Much debate has occurred since related to reporting exposures, near misses, and laboratory acquired infections.

9. Branswell, H. (February 2009). Baxter: Product contained live bird flu virus. *The Canadian Press.*

This newspaper articles provides an account of an incident involving the shipment of contaminated product from an Austrian research company to sub-contractors in Czech Republic, Slovenia and Germany. The material contained H3N2 seasonal viruses contaminated with H5N1 viruses. While no human exposures or infections resulted from the error, the potential consequences were of great concern, most notably the possibility of reassortment, although no evidence of such occurrence was observed.

10. Biosafety and SARS Incident in Singapore September 2003: Report of the Review Panel on New SARS Case and Biosafety (2003). World Health Organization, Geneva.

This report details the findings of an 11-member panel established at the request of the Singapore Ministry of Health in response to a laboratory acquired infection of SARS. A review of several BSL-3 laboratories in Singapore was also conducted to evaluate biosafety requirements and practices.

Many facility and programmatic deficiencies were noted by the expert panel. Most of the observations involved inadequate facility infrastructure, limited to no personnel training, insufficient biosecurity protocols, and a general lack of a culture of compliance and safety.

11. Martin-Mazuelos, E., et al. (1994). Outbreak of *Brucella melitnesis* among Microbiology Laboratory Workers. *Journal of Clinical Microbiology,* 32:8, 2035-2036.

This paper discusses an outbreak of laboratory-acquired brucellosis involving four laboratory technicians from a single microbiology laboratory during the summer of 1988. The investigation identified the probable source of infection was the handling of blood cultures. All four individuals worked in the same area where the cultures were handled and no accidents were reported to have occurred; however, the material was not handled or manipulated inside a biosafety cabinet. New policies and procedures were developed and implemented following the outbreak, most notably that all handling and manipulations of *Brucella* spp. were to be conducted inside a biosafety cabinet, and no new cases have been detected.

Biorisk Drivers

1. A Risk Management Standard (2002).The Institute for Risk Management, the Association of Insurance and Risk Managers, and the National Forum for Risk Management in the Public Sector, United Kingdom.

This paper describes the need for a risk management standard to ensure a consensus on terminology, processes, organizational structure, and objectives.

As it relates to drivers, the paper discusses the internal and external factors that form drivers of key risks. The drivers include strategic risks, operational risks, financial risks, and hazard risks. Further discussion of these elements is included in the section on Risk Analysis, the first step of Risk Assessment as defined by the ISO/IEC Guide 73.

2. An Introduction to the IRGC Risk Governance Framework (2008). International Risk Governance Council (IRGC), Geneva.

In this paper the IRGC puts forward an integrated analytic framework for risk governance and provides guidance for developing comprehensive assessment and management strategies to cope with risks. The framework integrates scientific, economic, social and cultural aspects and includes the effective engagement of stakeholders.

Risk governance comprises a broad picture of risk, and it includes what has been termed “risk management” and “risk analysis” as well as looking at how risk-

related decision making unfolds when a range of actors is involved, requiring coordination between a variety of roles, perspectives, goals and activities.

IRGC's risk governance framework comprises five linked phases: pre-assessment, appraisal, characterization and evaluation, management, and communication. As it relates to drivers, the risk pre-assessment phase is the most applicable and involves risk framing, early warning, screening, and determination of scientific conventions. The overall purpose of the pre-assessment phase is to capture both the variety of issues that stakeholders and society may associate with a certain risk (i.e. drivers) as well as existing indicators, routines, and conventions that may prematurely narrow down, or act as a filter for, what is going to be addressed as risk.

3. ISO 31000, Risk Management – Principles and Guidelines on Implementation (2009). ISO, Geneva.

This document is a group of standards that provides principles and generic guidelines on risk management. Its goal is to provide a universally recognized model for organizations employing risk management processes to replace the multitude of existing standards, methodologies and examples that typically differ between industries, subject matters, and regions. The ISO 31000 group includes ISO 31000, Principles and Guidelines on Implementation; IEC 31010, Risk Management – Risk Assessment Techniques; and ISO/IEC 73, Risk Management Vocabulary.

The driver-related steps of ISO 31000 involve establishing context, which is similar to the IRGC pre-assessment phase, including "risk framing". By establishing the context the organization defines the internal and external parameters to be taken into account when managing risk, and setting the scope and risk criteria for the remaining process. The context should include both internal and external parameters relevant for the organization. While many of these parameters are similar to those considered in the design of the risk management framework , when establishing the context for the risk management process, they need to be considered in greater detail and particularly how they relate to the scope of the particular risk management process.

External context is the external environment in which the organization seeks to achieve its objectives. Understanding the external context is important to ensure that external stakeholders, their objectives and concerns are considered when developing risk criteria. It is based on the organization wide context but with specific details of legal and regulatory requirements, stakeholder perceptions, and other aspects of risks specific to the scope of the risk management process. The external context can include, but is not limited to:

- the cultural, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;

- key drivers and trends having impact on the objectives of the organization; and
- perceptions and values of external stakeholders.

Internal context is the internal environment in which the organization seeks to achieve its objectives. The risk management process should be aligned with the organization's culture, processes and structure. Internal context is anything within the organization that can influence the way in which an organization will manage risk. It is necessary to understand the internal context, in terms of, for example:

- the capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);
- information systems, information flows, and decision making processes (both formal and informal) ;
- internal stakeholders;
- policies, objectives, and the strategies that are in place to achieve them;
- perceptions, values and culture; and
- standards and reference models adopted by the organization.
- structures (e.g. governance, roles and accountabilities).

Biorisk Monitoring

Al-Hemoud, A. M., & Al-Asfoor, M. M. (2006). A behavior based safety approach at a Kuwait research institution. *Journal of Safety Research , 37*, 201-206.

Alvero, A. M., Rost, K., & Austin, J. (2008). The safety observer effect: The effects of conducting safety observations. *Journal of Safety Research , 39*, 365-373.

Aven, T. (2009). Safety is the antonym of risk for some perspectives of risk. *Safety Science , 47*, 925-930.

Baram, M. (2009). Biotechnological research on the most dangerous pathogens: Challenges for risk governance and safety management. *Safety Science , 47*, 890-898.

Biddle, E., Ray, Ray, T., Owusu-Edusei, J. K., & Camm, T. (2005). Synthesis and recommendations of the economic evalution of OHS interventions at the company level conference. *Journal of Safety Research - ECON proceedings , 36*, 261-267.

Blavier, A., Rouy, E., Nyssen, A.-S., & De Keyser, V. (2005). Prospective issues for error detection. *Ergonomics , 48* (7), 758-781.

Burnett, L. C. (2006). Biological Safety Program Management. In D. O. Fleming, & D. L. Hunt (Eds.), *Biological Safety: Principles and Practices* (pp. 405-415). Washington, D.C., USA: ASM Press.

Celik, M. (2009). Designing of integrated quality and safety management system (IQSMS) for shipping operations. *Safety Science , 47*, 569-577.

Choudry, R. M., Fang, D., & Mohamed, S. (2007). Developing a Model of Construction Safety Culture. *Journal of Management in Engineering , 23* (4), 207-212.

Clarke, S. (2006). Contrasting perceptual, attitudinal and dispositional approaches to accident involvement in the workplace. *Safety Science , 44*, 537-550.

Coghlan, K. (2008, January). Investigating Laboratory Accidents. *Safety Professional* , 56-57.

Cooper, M., & Phillips, R. (2004). Exploratory analysis of the safety climate and safety behavior relationship. *Journal of Safety Research , 35*, 497-512.

DeJoy, D. M. (2005). Behavior change versus culture change: Divergent approaches to managing workplace safety. *Safety Science , 43*, 105-129.

DeJoy, D. M. (1996). Theoretical Models of Health Behavior and Workplace Self-Protective Behavior. *Journal of Safety Research , 27* (2), 61-72.

DeJoy, D. M., Gershon, R. R., & Schaffer, B. S. (2004, July). Safety Climate: Assessing management and organizational influences on safety. *Professional Safety*, 50-57.

DeJoy, D. M., Murphy, L. R., & Gershon, R. M. (1995). The influence of employee, job/task, and organization factors on adherence to universal precautions among nurses. *International Journal of Industrial Ergonomic , 16*, 43-55.

DeJoy, D. M., Schaffer, B. S., Wilson, M. G., Vandenberg, R. j., & Butts, M. M. (2004). Creating safety workplaces: assessing the determinants and role of safety climate. *Journal of Safety Research , 35*, 81-90.

DeJoy, D. (2008). Managing Biosafety: Facilitating Incident Reporting. *Biosafety and Laboratory Incident Reporting Workshop. January 30, 2008.* Atlanta, GA: Southeast Regional Centers of Excellence in Biodefense and Emerging Diseases Policy, Ethics, and Law Core.

DeVries, J. E., Burnette, M. M., & Redmon, W. K. (1991). AIDS Prevention: Improving Nurses' Compliance with glove wearing through performance feedback. *Journal of Applied Behavior Analysis , 24* (4), 705-711.

Diaz, R. I., & Cabrera, D. D. (1997). Safety climate and attitude as evaluation measures of organizational safety. *Accident Analysis and Prevention , 29* (5), 643-650.

Eherts, D. M. (2008). Lessons Learned from Aviation Safety. *Journal of Safety Research , 39*, 141-142.

Fernandez-Muniz, B., Montes-Peon, J. M., & Vazquez-Ordas, C. J. (2007). Safety Culture: Analysis of the causal relationships between its key dimensions. *Journal of Safety Research , 38*, 627-641.

Flin, R., Mearns, K., O'Connor, P., & Bryden, R. (2000). Measuring safety climate: identify the common features. *Safety Science , 34*, 177-192.

Fullarton, C., & Stokes, M. (2007). The Utility of a workplace injury instrument in predication of workplace injury. *Accident Analysis and Prevention , 39*, 28-37.

Geller, E. S., Perdue, S. R., & French, A. (2004, July). Behavior-based Safety Coaching. *Professional Safety* , 42-49.

Gershon, R. R., Karkashian, C. D., Grosch, J., Murphy, L. R., Escamilla-Cejudo, A., Flanagan, P. A., et al. (2000). Hospital safety climate and its relationship with safety work practices and workplace exposure incidents. *American Journal of Infection Control , 28* (3), 211-221.

Glendon, A., & Litherland, D. (2001). Safety climate factors, groups differences and safety behaviour in road construction. *39*, 157-188.

Gordon, R., Flin, R., & Mearns, K. (2005). Designing and evaluating a human factors investigation tool (HFIT) for accident anaylsis. *Safety Science , 43*, 147-171.

Gordon, R., Kirwan, B., & Perrin, E. (2007). Measuring safety culture in a research and development centre: A comparison of two methods in the Air Traffic Management domain. *Safety Science , 45*, 669-695.

Griffin, M. A., & Neal, A. (2000). Perceptions of Safety at Work: A Framework for Linking Safety Climate to Safety Performance, Knowledge, and Motivation. *Journal of Occupational Health Psychology, 5* (3), 347-358.

Hahn, S. E., & Murphy, L. R. (2008). A short scale for measuring safety climate. *Safety Science , 46*, 1047-1066.

Havold, J. I. (2005). Safety-culture in a Norwegian shipping company. *Journal of Safety Research , 36*, 441-458.

Hoffman, D. A., & Stetzer, A. (1998). Role of Safety Climate and Communication in Accident Interpretation: Implications for Learning from Negative Events. *The Academy of Management Journal , 41* (6), 644-657.

Hoogendorn, M., Jonker, C. M., Treur, J., & Verhaergh, M. (2009). Agent-based analysis and support for incident management. *Safety Science , 47*, 1163-1174.

Huang, Y.-H., Chen, J.-C., DeArmond, S., Cigularov, K., & Chen, P. Y. (2007). Roles of safety climate and shift work on perceived injury risk: A multi-level analysis. *Accident Analysis and Prevention , 39*, 1088-1096.

Huang, Y.-H., Ho, M., Smith, G. S., & Chen, P. Y. (2006). Safety climate and self-reported injury: Assessing the mediating role of employee safety control. *Accident Analysis and Preventtion , 38*, 425-433.

Jovasevic-Stojanovic, M., & Stonjanovic, B. (2009). Performance Indicators for Monitoring Safety Management Systems in Chemical Industry. *Chemical Industry & Chemical Engineering Quarterly , 15* (1), 5-8.

Katsakiori, P., Sakellaropoulos, G., & Manatakis, E. (2009). Towards and evalution investigation methods in terms of their alignment with accident causation models. *Safety Science , 47*, 1007-1015.

Kelly, B., & Berger, S. (2006). Interface management: Effective communication to improve process safety. *Journal of Hazardous Materials , 130*, 321-325.

Kletz, T. (2002). Accident Investigation - Missed Opportunities. *Trans IChemE , 80* (Part B), 3-8.

Kontogiannis, T., & Malakis, S. (2009). A proactive approach to human error detection and identification in aviation and air traffic control. *Safety Science , 47*, 693-706.

Langerman, N. (2009, July/August). Lab-scale process safety management. *Journal of Chemical Health & Safety* , 22-28.

Le Coze, J.-c. (2008). Disasters and organisations: From lessons learnt to theorising. *46*, 132-149.

Lu, C.-S., & Shang, K.-c. (2005). An empirical investigation of safety climate in container terminal operators. *Journal of Safety Research , 36*, 297-308.

Lundberg, J., Rollenhagen, C., & Hollnagel, E. (2009). What-You-Look-For-Is-What-You-Find - The consequences of underlying accident models in eight accident investigation manuals. *Safety Science , in press*.

Luria, G., & Rafaeli, A. (2008). Testing safety commitment in organization through interpretations of safety artifacts. *Journal of Safety Research , 39*, 519-528.

Luria, G., Zohar, D., & Erev, I. (2008). The effect of workers' visibility of effectiveness of intervention programs: Supervisory-based safety interventions. *Journal of Safety Research , 39*, 273-280.

Modica, M. (2007, July). Safe Science: Applying safety in a modern research laboratory. *Professional Safety* , 24-30.

Montero, M. J., Araque, R. A., & Rey, J. M. (2009). Occupational health and safety in the framework of corporate social responsibiity. *Safety Scinece , in press*.

Mure, S., & Demichela, M. (2009). Fuzzy Application Procedure (FAP) for the risk assessment of occupational accidents. *Journal of Loss Prevention in the Process Industries , 22*, 593-599.

Neal, A., & Griffin, M. A. (2006). A Study of the Lagged Relationships Among Safety Climate, Safety Motivation, Safety Behavior, and Accidents at the Individual and Group Levels. *Journal of Applied Psychology, 91* (4), 946-953.

Neal, A., Griffin, M., & Hart, P. (2000). The impact of organizational climate on safety climate and individual behavior. *Safety Science , 34*, 99-109.

OECD Environment Directorate. (2008). *Guidance on Developing Safety Performance Standards related to Chemical Accident Prevention, Preparedness and Response* (Vol. No. 19). Paris, France: OECD Environment, Health, and Safety Publications.

Olson, R., & Austin, J. (2001). Behavior-based safety and working along: The effects of a self-monitoring package on the safe performance of bus operators. *Journal of Organizational Behavior Management , 21* (3), 5-43.

Parker, D., Brosseau, L., Samant, Y., Pan, W., Xi, M., Haugan, D., et al. (2007). A comparison of the perceptions and beliefs of workers and owners with regard to workplace safety in small metal fabrication businesses. *American Journal of Industrial Medicine , 50*, 999-1009.

Pransky, G., Synder, T., Dembe, A., & Himmelstein, J. (1999). Under-reporting of work-related disorders in the workplace: a case study and review of the literature. *Ergonomics, 42* (1), 171-182.

Probst, T., Brubaker, T. L., & Barsotti, A. (2008). Organizational Injury Rate Underreporting: The Moderating Effect of Organizational Safety Climate. *Journal of Applied Psychology, 93* (5), 1147-1154.

Prussia, G. E., Brown, K. A., & Willis, P. G. (2003). Mental models of safety: do managers and employees see eye to eye? *Journal of Safety Research, 34*, 143-156.

Reinach, S., & Viale, A. (2006). Application of a human error framework to conduct train accident/incident investigations. *Accident Analysis and Prevention, 38*, 396-406.

Reniers, G., Ale, B., Dullaert, W., & Soudan, K. (2009). Designing continuous safety improvement within chemical industrial areas. *Safety Science , 47*, 578-590.
Rundmo, T. (1997). Associations between risk perception and safety. *Safety Science, 24* (3), 197-209.

Shannon, H. S., Mayr, J., & Haines, T. (1997). Overview of the relationship between organizational and workplace factors and injury rates. *Safety Science, 26* (3), 201-217.

Shannon, H. s., Robson, L. S., & Guastello, S. J. (1999). Methodological criteria for evaluation occupational safety intervention research. *Safety Science, 31*, 161-179.

Sklety, S. (2004). Comparison of some selected methods for accident investigation. *Journal of Hazardous Materials, 111*, 29-37.

Smith, G. S., Huang, Y.-H., Ho, M., & Chen, P. Y. (2006). The relationship between safety climate and injury rates across industries: The need to adjust for injury hazards. *Accident Analysis and Prevention, 38*, 556-562.

Stoop, J., & Roed-Larsen, S. (2009). Public safety investigations - A new evolutionary step in safety enhancement? *Reliability Engineering and System Safety, 94*, 1471-1479.

Turnberg, W., & Daniell, W. (2008). Evaluation of a healthcare safety climate measurement tool. *Journal of Safety Research, 39*, 563-568.

Vrendenburgh, A. G. (2002). Organizational Safety: Which management practices are most effective in reducing employee injury rates? *Journal of Safety Research, 33*, 259-276.

Vrijling, J., van Hengel, W., & Houben, R. (1995). A framework for risk evaluation. *Journal of Hazardous Materials, 43*, 245-261.

Wallace, J. C., Little, L. M., & Shull, A. (2008). The Moderating Effects of Task Complexity on the Relationahip Between Regulatory Foci and Safety and Production Performance. *Journal of Occupational Health Psychology, 13* (2), 95-104.

Wirth, O., & Sigurdsson, S. O. (2008). When workplace safety depends on behavior change: Topics for behavioral safety research. *Journal of Safety Research, 39*, 589-598.

Wu, T.-C. (2008). Safety leadership in the teaching laboratories of electrical and electronic engineering departments at Taiwanese Universities. *Journal of Safety Research, 39*, 599-607.

Wu, T.-C., Chen, C.-H., & Li, C.-C. (2008). A correlation among safety leadership, safety climate and safety performance. *Journal of Loss Prevention in the Process Industries, 21*, 307-318.

Wu, T.-C., Li, C.-C., Chen, C.-H., & Shu, C.-M. (2008). Interaction effects of organization and individual factors on safety leadership in college and univesity laboratories. *Journal of Loss Prevention in the Process Industries, 21*, 239-254.

Wu, T.-C., Liu, C.-W., & Lu, M.-C. (2007). Safety climate in university and college laboratories: Impact of organization and individual factors. *Journal of Safety Research, 38*, 91-102.

Biorisk Sustainability

1. Expert forecast on emerging biological risks related to safety and health (2007). European Risk Observatory Report. http://osha.europa.eu//en/publications/reports/7606488/

This report contains a forecast of emerging biological risks related to occupational safety and health (OSH) based on an expert survey and a literature review. The European Agency for Safety and Health at Work also worked on forecasts and literature reviews on physical, chemical, and psychosocial risks in order to paint as full a picture as possible of the potential emerging risks in the world of work.

Behind the top emerging biological risk identified in the report, occupational risks related to global epidemics, followed risks resulting from poor risk assessment. Ongoing management of biological risks based on proper assessment appears as one of the main issues for the sustainability of biorisk management.

2. White paper on Risk Governance (2006). The International Risk Governance Council. http://www.irgc.org/The-IRGC-risk-governance-framework.82.html

See Item 2 under the Biorisk Drivers above.

As it relates to biorisk sustainability, this paper describes risk governance as providing a framework for an organization to enable activities to take place in a sustainable manner. The risk governance model aims to improve decision making, planning and prioritization, thus contributing to a more efficient allocation and use of the resources within an organization. This process creates value by ensuring the resources consumed by risk management and control are used efficiently to

guarantee the sustainability of the activities and the achievement of the organization's strategic objectives.

3. Laboratory Biorisk Management Standard (2008), CWA 15793:2008. ftp://ftp.cenorm.be/PUBLIC/CWAs/workshop31/CWA15793.pdf.

This document describes a laboratory biorisk management standard that aims to set requirements necessary to control risks associated with the handling or storage and disposal of biological agents and toxins in laboratory facilities, regardless of type, size or biological agents handled. The central theme of the standard is the risk assessment.

The general approach to a biological risk assessment involves hazard identification and risk analysis of the activities which results in a determination of appropriate biological containment level and any special practices or procedures to enhance the protection of personnel, the community and the environment. However, more often elements such as biosecurity, public perception, operating costs, or risk acceptance level are generally not considered in the typical biological risk assessment approach. The laboratory biorisk management standard aims to bridge these gaps and provide a more sustainable model not only for the planning phase, which includes the risk assessment, but also for more effective implementation of the decisions made and ongoing monitoring of their outcome.

Other Biorisk Management Issues

Physical security

1. Garcia, M. L. (2001). *The Design and Evaluation of Physical Protection Systems*. Burlington, MA: Butterworth-Heinemann, Print.

During the initial considerations for the implementation of a physical protection system (PPS), the facility must be characterized so that an appropriate level of protection can be determined. The facility should be characterized according to physical conditions, facility operations, facility policies, procedures and training, regulatory requirements, legal issues such as security liability and failure to protect, safety considerations, and corporate objectives. Regulatory requirements include those from the fire department, safety and health regulators, federal government agencies including the Departments of Labor, Energy, Defense, and Commerce, and special regulatory agencies such as the Nuclear Regulatory Commission and the International Atomic Energy Agency. Since a potentially significant investment must be made in the implementation of a PPS, it is also critical that senior management view an effective security system as essential for business operation.

2. The Physical Protection of Nuclear Material and Nuclear Facilities INFCIRC/225/Rev.4 (Corrected)

The objectives of the International Atomic Energy Agency (IAEA) are to provide a set of recommendations on requirements for the physical protection of nuclear material in use and storage and during transport and of nuclear facilities. The recommendations are provided for consideration by the competent authorities in the States. The INFCIRC/225/Rev.4 document obligates parties to the following: define specific standards of physical protection for international shipments of nuclear material; co-operate in the recovery and protection of stolen nuclear material; make specified acts to misuse or threats to misuse nuclear materials to harm the public criminal offenses, and prosecute or extradite those accused of committing such acts. The primary factor for determining the physical protection measures against unauthorized removal of nuclear material is the nuclear material itself, which is categorized in accordance with a table published in the IAEA document.

3. U.S. Department of Energy, O 470. 4A, Safeguards and Security Program.

This directive defines a basis for security system design standards and facility and physical protection standards. It mandates that DOE assets be protected from theft or diversion, sabotage, espionage, and other acts that could have high-consequence impacts on national security, program continuity, or the health and safety of employees, the public, or the environment. Implementing protection should provide effective security while maintaining compliance while balancing project cost, potential safety concerns, and operational impacts.

4. U.S. Department of Energy M 470. 4 Series of Manuals.

These manuals contain requirements for determining the level of protection, based on facility functions and design basis threat requirements. DOE assets are defined and protection standards outlined in DOE O 470.3A, Design Basis Threat Policy. Depending on the asset, protection strategies range from compliance with DOE security policies to specific performance standards that should be met. This constitutes a graded, risk-based approach ensuring the highest levels of protection for those assets where loss, theft, compromise, and/or unauthorized use would seriously affect national security, DOE programs, and/or the health and safety of employees, the public, or the environment.

5. Director of Central Intelligence Directives 6/9, Physical Security Standards for Sensitive Compartmented Information Facilities.

This manual establishes physical security standards for the protection of facilities where Sensitive Compartmented Information (SCI) is stored, processed and discussed. It includes a policy and specifications for the construction of Sensitive Compartmented Information Facilities (SCIFs).

6. Unified Facilities Criteria, Department of Defense Minimum Antiterrorism Standards for Buildings.

The Unified Facilities Criteria (UFC) requires DoD components to adopt common security criteria and construction standards to mitigate vulnerabilities to terrorist threats. The document provides planning, design, construction, sustainment, restoration, and modernization criteria.

7. Department of Justice Vulnerability Assessment of Federal Buildings

The Department of Justice conducted this study on the vulnerability of federal office buildings to acts of terrorism and other forms of violence. As part of the study, a standards committee developed 52 security standards on subjects such as perimeter parking, lighting, and physical barriers. Federal sites were divided into five security levels ranging from a Level 1 with minimum security needs to a Level 5. For higher-security level buildings, the report calls for further controls such as perimeter monitoring by closed-circuit television, intrusion-detection systems, x-ray screening of mail, the installation of shatter-proof glass on exterior windows, and a set-back from the street for new buildings.

Training frequency

1. Arthur, W., et al. (1998) Factors That Influence Skill Decay and Retention: A Quantitative Review and Analysis. *Human Performance* 11.1 57-101. Print.

2. Ginzburg, S. & Dar-El, E., 2000: Skill retention and relearning – a proposed cyclical model. In: *Journal of Workplace Learning*, 12: 327-332.

3. (DTIC No. ADA163710) Loftus, G. R. (1985). Evaluating forgetting curves. *Journal of Experimental Psychology: Learning, Memory, & Cognition*, 9, 730-746.

Enterprise risk management

1. Enterprise Risk Management – Integrated Framework: Executive Summary (September 2004). Committee of Sponsoring Organizations (COSO) of the Treadway Commission, PricewaterhouseCoopers, New York.

This paper describes the essential components, principles and concepts of enterprise risk management for all organizations, regardless of size. As defined by COSO, enterprise risk management (ERM) is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the

entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives. These objectives can be viewed in the context of four categories: strategic, operations, financial reporting and compliance, all of which are very similar to the IRGC risk governance framework described above. Just as with all risk management strategies, the centerpiece of ERM is the risk assessment and subsequent response and control. Additional aspects also taken into account communication and ongoing monitoring activities, which are key components of the CEN's Laboratory Biorisk Management Standard.

2. Overview of Enterprise Risk Management (May 2003). Enterprise Risk Management Committee, Casualty Actuarial Society (CAS).

This document is primarily a study guide for professionals serving in the actuarial sciences; however, it does provide an interesting history and evolution for enterprise risk management (ERM), most notably by looking at the internal (i.e. competitive advantage) and external (i.e. corporate governance) pressures driving the ERM movement.

Policy issues

1. Enhancing Personnel Reliability Among Individuals with Access to Select Agents (May 2009). National Science Advisory Board for Biosecurity. Bethesda, MD.

This report describes the findings of the NSABB and its efforts to identify strategies for enhancing personnel reliability among individuals with access to select agents and toxins (i.e. the "insider threat"). Research programs that have utilized materials that are deemed sensitive from a national security perspective (i.e., nuclear and chemical weapons programs) have addressed the insider threat as a component of larger "surety" programs. Surety programs contain features aimed at ensuring that the materials are physically secure, safely handled, and properly inventoried. Surety programs also have formal personnel reliability components to help ensure that the individuals with access to sensitive materials are trustworthy and reliable. These formal Personnel Reliability Programs (PRPs) may include background investigations, security clearances, medical examinations, psychological evaluations, polygraph testing, drug and alcohol screening, credit checks, and systems of ongoing monitoring.

Although the risk of the insider threat is uncertain, it is likely quite small based on history. Even in the open climate that is the hallmark of most life sciences research, the overwhelming majority of such research – including select agent research – has been conducted by responsible researchers toward commendable aims. The potential benefits of enhanced personnel reliability measures must be carefully weighed against the potential negative consequences that such measures would likely have on the research community. The promulgation of additional reliability

measures could serve as a powerful disincentive to those who wish to and would responsibly conduct research on select agents because the most talented young researchers, those with many options for research paths, may be far more likely to enter fields with less onerous regulatory requirements. Thus, a burdensome national personnel reliability program may not only drive scientists from important select agent research, but also drive select agent research out of academia and potentially out of the U.S. into countries with less stringent regulations.

2. Biological Safety Training Programs as a Component of Personnel Reliability (May 2009). American Association for the Advancement of Science. Washington, DC.

The main area of focus of this report was to address shortcomings and challenges in designing and implementing biosafety training programs. The findings of the AAAS group identified several needs including applied biosafety research, exposure reporting mechanisms, and competency standards. As it relates to personnel reliability, the group recommended that current employment and biosafety practices in various organizations may already address concerns over personnel reliability and that implementation of a formal personnel reliability program may be too costly for the non-governmental sector.

3. Report to Congressional Requestors - High Containment Laboratories; National Strategy for Oversight is Needed (September 2009). U.S. Government Accountability Office, Washington, DC.

4. Report of the Trans-Federal Task Force on Optimizing Biosafety and Biocontainment Oversight (September 2009) Co-chaired by U.S. Department of Health and Human Services and U.S. Department of Agriculture.

5. World at Risk: The Report of the Commission on the Prevention of WMD Proliferation and Terrorism (December 2008). http://www.preventwmd.gov/report/

The commission that released this report was established by the U.S. Congress in 2007 in response to a recommendation in the 9/11 Commission Report and was chaired by former U.S. Senator Bob Graham. One area of focus for the Graham Commission related to biorisk involves the development of a new blueprint to prevent biological weapons proliferation and bioterrorism. In this regard the Commission made the following recommendations:

- HHS should lead an interagency review of the domestic program to secure dangerous pathogens
- DHS should take the lead in developing a national strategy for advancing microbial forensics capabilities

- HHS and DHS should lead an interagency effort to tighten government oversight of high-containment laboratories
- HHS and Congress should promote a culture of security awareness in the life sciences community
- HHS and DHS should take steps to enhance the nation's capacity for rapid response to prevent an anthrax attack from inflicting mass casualties
- DOS and HHS should press for an international conference of countries with major biotechnology industries
- DOS should lead a global assessment of biological threats and engage in targeted biological threat prevention programs in additional countries
- HHS, through CDC, should work to strengthen global disease surveillance networks
- United States should reaffirm the critical importance of the BWC

Of these, the first, third and fourth recommendations have specific biorisk management implications and provide support for the development and implementation of an effective biorisk management system which would likely address the key elements of these recommendations.