CEN

WORKSHOP

AGREEMENT

CWA 16393

January 2012

ICS 07.100.01

English version

Laboratory biorisk management - Guidelines for the implementation of CWA 15793:2008

This CEN Workshop Agreement has been drafted and approved by a Workshop of representatives of interested parties, the constitution of which is indicated in the foreword of this Workshop Agreement.

The formal process followed by the Workshop in the development of this Workshop Agreement has been endorsed by the National Members of CEN but neither the National Members of CEN nor the CEN-CENELEC Management Centre can be held accountable for the technical content of this CEN Workshop Agreement or possible conflicts with standards or legislation.

This CEN Workshop Agreement can in no way be held as being an official standard developed by CEN and its Members.

This CEN Workshop Agreement is publicly available as a reference document from the CEN Members National Standard Bodies.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

Management Centre: Avenue Marnix 17, B-1000 Brussels

© 2012 CEN All rights of exploitation in any form and by any means reserved worldwide for CEN national Members.

Ref. No.:CWA 16393:2012 E

Contents

Page

Foreword

This CEN Workshop Agreement has been drafted and approved by a Workshop of representatives of interested parties on 2011-11-25, the constitution of which was supported by CEN following the public call for participation made on 2010-01-13. NEN, the Netherlands Standardization Institute, provided the secretariat of the Workshop.

A list of the individuals and organizations which supported the technical consensus represented by the CEN Workshop Agreement is available to purchasers from the CEN-CENELEC Management Centre. These organizations were drawn from the following organisations: Aga Khan University, PK, American Biological Safety Association (ABSA), Animal Health Research Centre, ES, Asia-Pacific Biosafety Association (A-PBA), SG, Azerbaijan Medical University, AZ, Bayer CropScience, BE, Biological Threat Reduction Program, US, Biosecurity Institute, DK, Boston University and Boston Medical Center, US, Centers for Disease Control and Prevention, KR, Deakin University, AU, Defense Threat Reduction Agency, US, Det Norske Veritas (DNV), NO, E.R. Griffin Research Foundation, US, Eliava Institute, GE, Emory University, US, European Biosafety Association (EBSA), Friedrich-Loeffler-Institut, Federal Research Institute for Animal Health, DE, GlaxoSmithKline Biologicals, BE, Global Partnership Program, CA, Hannover Medical School, DE, Institute for Animal Health, GB, Institute for Medical Research Ministry of Health, MY, International Centre for Infectious Diseases, CA, Kazakhstan Scientific Center of Quarantine and Zoonotic Diseases, KZ, Kenya Medical Research Institute (KEMRI), KE, KESC Medical, PK, Laboratory of Ministry of Agriculture (LMA), GE, Medical Biological Safety Association, MX, Medical Research Council (MRC), GB, Merck Sharp & Dohme, US, Ministry of Health, AZ, Ministry of Health, PH, National Center for Disease Control and Public Health (NCDC&PH), GE, National Institute for Public Health and the Environment, NL, National Institute of Health Research and Development, ID, National Institute of Public Health, RO, National Institutes of Health, US, National Veterinary Laboratory, PK, Novartis International AG, CH, Pfizer, IE, Plas-Labs, US, Public Health Agency of Canada, CA, Regional Public Health Department, GE, Republican Veterinary Laboratory, AZ, Research Institute for Biological Safety Problems, KZ, San Lazaro Hospital, PH, Sandia National Laboratories, US, SES, UA, Société Général de Surveillance (SGS), CH, Spiez laboratory, CH, Statens Serum Institut, DK, Telstar Projects (Tpro), ES, U.S. Government Accountability Office, US, Universidad Autónoma de Madrid, ES, US Department of State, US, US Naval Medical Research Unit, US, WHO collaborating Center for Biosafety in Microbiology, AU, World BioHazTec Corporation, US, Xibios, BE.

The formal process followed by the Workshop in the development of the CEN Workshop Agreement has been endorsed by the National Members of CEN but neither the National Members of CEN nor the CEN-CENELEC Management Centre can be held accountable for the technical content of the CEN Workshop Agreement or possible conflict with standards or legislation. This CEN Workshop Agreement can in no way be held as being an official standard developed by CEN and its members.

The final review/endorsement round for this CWA was started on 2011-11-07 and was successfully closed on 2011-11-25.The final text of this CWA was submitted to CEN for publication on 2011-12-02.

Background

CWA 15793:2008 - Laboratory Biorisk Management Standard - was developed as a voluntary standard by an international consortium of biosafety and biosecurity experts through a CEN Workshop (WS 31) to describe the required components of an effective biorisk management system. To facilitate implementation of CWA 15793, this guidance document has been developed to build on and expand the guidance notes already provided.

Because CWA 15793:2008 is compatible with management guidance documents, such as ISO 9000 series (Quality), ISO 14000 series (Environmental), OHSAS 18000 series (Health and Safety) and BSI PAS 99 integrated management series, it can be integrated with them.

Format

The document quotes the specific requirements from CWA 15793:2008 in a framed text box accompanied in many cases with informative guidance notes to aid interpretation. Guidance notes from CWA 15793:2008 are in italics; if notes have been expanded for clarification or to remove redundancies, the text is not in italics. The clause numbering of the document is aligned with that of CWA 15793:2008. In the event the output is identical to the intent, only the intent will be stated.

Generic guidance is provided on the application and implementation of CWA 15793:2008. The underlying principles of CWA 15793:2008 are explained against each requirement. This document does not create additional requirements to those specified in CWA 15793:2008 nor does it prescribe mandatory approaches to the implementation of CWA 15793:2008. To be consistent with other management systems, where appropriate, the text will address intent, typical input and output without explicitly referring to these terms.

The new guidance document should not conflict with the notes provided in CWA 15793:2008; however, if there are areas where different interpretation is possible, the text provided by CWA 15793:2008 will take precedence.

This CEN Workshop Agreement is publicly available as a reference document from the National Members of CEN: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Comments or suggestions from the users of the CEN Workshop Agreement are welcome and should be addressed to the CEN-CENELEC Management Centre.

Introduction

Organizations of all kinds are increasingly concerned with achieving and demonstrating robust biosafety and biosecurity practices controlling their biorisks consistent with their own biorisk policy and objectives. They do so in the context of increasing concern expressed by a variety of stakeholders and, in many countries, by a regulatory system that is becoming increasingly stringent.

Many organizations have undertaken biorisk “reviews” or “audits” to assess their biorisk performance. On their own, however, these “reviews” and “audits” may not be sufficient to provide an organization with the assurance that its performance not only meets, but also will continue to meet, its legal and policy requirements. To be effective, they need to be conducted within a structured systematic approach integrated throughout the organization.

CWA 15793:2008 specifies requirements for a biorisk management system that will enable an organization to develop and implement a biorisk policy, establish objectives and processes to achieve the policy commitments and improve its performance. It follows a risk based approach taking in legal requirements and current knowledge and is intended to apply to all types and sizes of organizations and to accommodate diverse geographical, cultural and social conditions. The success of the system depends on commitment from all levels and functions within the organization, and especially from top management. The overall aim of CWA 15793:2008 is to support and promote good biorisk practices, including self regulation.

This guidance is in the form of notes in association with the pertaining requirements clause and uses the terms “should” (recommendation), “may” (allowance) and “can” (possibility). Organizations wishing to implement this CWA 15793:2008 would be expected to consider all recommendations where the term “should” is used.

The management system approach enables an organization to effectively identify, monitor and control the laboratory biosafety and biosecurity aspects of its activities.

An effective management system approach should be built on the concept of continual improvement through a cycle of planning, implementing, reviewing and improving the processes and actions that an organization undertakes to meet goals. This is known as the PDCA (Plan-Do-Check-Act) principle:

Plan: Planning, including identification of hazard and risk and establishing goals,

Do: Implementing, including training and operational issues,

Check: Checking, including monitoring and corrective action,

Act: Reviewing, including process innovation and acting to make needed changes to the management system.

This document was written as a guide to the CWA 15793:2008 Laboratory biorisk management standard, wich aims to support organizations and biosafety professionals to implement a biorisk management system that is both practicable and robust.

1 Scope

For the purposes of this document, the scope given in the CWA 15793:2008 Laboratory biorisk management standard, applies to this guidance document.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

CWA 15793:2008, *Laboratory biorisk management standard*

NOTE In 2011, the workshop 31 participants renewed the CWA 15793:2008 for another three years without any technical changes. The only editorial changes implemented involved the replacement of the word “standard” in the original document with the words “CWA” or “Agreement” wherever appropriate, based on a request to CEN by the CEN National Members. Therefore, the application of this guidance document is relevant to CWA 15793:2011 as well.

3 Terms and definitions

For the purposes of this document, the terms and definitions given in CWA 15793:2008 apply.

4 Biorisk management system

4.1 General requirements

4.1.1 Biorisk management system

The organization shall establish, document, implement and maintain a biorisk management system in accordance with the requirements of this laboratory biorisk management standard.

This CWA 15793:2008 requirement is a general statement concerning the establishment and maintenance of a biorisk management system within an organization. “Establish” implies a level of permanency, and the system should not be considered established until all its elements have been demonstrably implemented. “Maintain” implies that, once established, the system continues to operate. This requires active effort on the part of the organization. The elements of CWA 15793:2008 (such as self-audit programme and corrective action and management review) aim to ensure proactive maintenance of the system.

The priority should be on protecting employees, their community and environment from accidental or unauthorized intentional release of biological materials from the facility.

The level of detail and complexity of the biorisk management system, the extent of documentation and the resources devoted to it will be dependent on the nature (size, structure, complexity) of an organization and its activities.

An organization may choose to implement CWA 15793:2008 for its entire facility or specific units or laboratories as long as any boundaries set do not exclude specific activities that have an impact on biorisk management for those units or laboratories implementing CWA 15793:2008.

Establishing a biorisk management system should consider the following:

— policy and objectives relevant to the organization's business as a whole;

— legal and other requirements;

— historical and current performance by the organization;

— needs of other interested parties;

— opportunities and need for continual improvement;

— resources needed;

— contributions of employees;

— contributions of contractors and other external personnel; and

— integrations with the specific requirements of e.g. ISO 9001, ISO 14001, ISO 15189:2007, ISO 17025, ISO/IEC 27001, ISO 22000, ISO/IEC 20000, ILO-OSH 2001, OHSAS 18001, and PAS 99:2006 (for more information see Bibliography).

An organization seeking to establish a biorisk management system that conforms to CWA 15793:2008 should determine its current position with regard to its biorisk by undertaking an initial review. In determining how it will fulfill the requirements of CWA 15793:2008, the organization should consider the conditions and factors that may affect how it will manage the biosafety and / or biosecurity of the facility.

4.1.2 Continual improvement

The organization shall continually improve the effectiveness of the biorisk management system through the use of the policy, objectives, self-audit programme, audit results, analysis of data, risk assessment, corrective and preventive actions and the management review.

The organization should strive to continue to develop and refine the systems in place to ensure that further opportunities to improve are identified and implemented. This may be achieved through goal setting and targets placed upon those working within the facility and monitoring progress to ensure the goals are achieved.

4.2 Policy

4.2.1 Biorisk management policy

The organization's top management shall develop, authorize, and sign a policy concerning the management of laboratory biorisk (laboratory biosafety and laboratory biosecurity). It shall clearly state the overall biorisk management objectives and a commitment to improving biorisk management performance.

The policy shall be appropriate to the nature and scale of the risk associated with the facility and associated activities and commit to:

a) protecting staff, contractors, visitors, community and environment from biological agents and toxins that are stored or handled within the facility;

b) reducing the risk of unintentional release of, or exposure to biological agents and toxins;

c) reducing the risk to an acceptable level of unauthorized intentional release of hazardous biological materials, including the need to conduct risk assessments and implement the required control measures;

d) complying with all legal requirements applicable to the biological agents and toxins that will be handled or possessed, and with the requirements of this standard;

e) ensuring that the need for effective biorisk management shall take precedence over all non "health and safety" operational requirements;

f) effectively informing all employees and relevant third parties and communicating individual obligations with regard to biorisk to those groups;

g) continually improving biorisk management performance.

This biorisk policy should be an integral part of the organization in establishing an overall sense of direction and sets the principles for biorisk management within the organization. The policy should set organizational objectives for biorisk and delineate roles and responsibilities for safety and security. It demonstrates that the organization and top management are committed to implementing and monitoring an effective biorisk management system.

Biorisk management should be stated clearly as part of the organization's health, safety and environment (HSE) policies. Depending on the relevance of biorisk management to the organization, the biorisk management policy should complement the general HSE policies. As appropriate, the biorisk management policy may be integrated into the organization's HSE policies. The policy should require all relevant *projects / work areas to be assessed for* biological *risks and a full assessment prepared before work is approved to commence.* Biosafety may be integrated to a general safety system, if appropriate.

When developing the policy, the organization should consider:

— the organization's mission, vision, core values and beliefs;

— the biological materials used or potentially used by the organization;

— coordination with other policies (corporate, Health Safety and Environment (HSE), etc.);

— the needs of persons working under the control of the organization;

— legal and other requirements to which the organization subscribes that relate to its biohazards;

— historical and current biorisk performance by the organization;

— opportunities and needs for continual improvement and the control of biorisks;

— the views of stakeholders; and

— what is needed to establish realistic and achievable objectives.

The responsibility for defining and authorizing a biorisk policy is the responsibility of the organization's top management. The ongoing and proactive involvement of top management in developing and implementing a biorisk policy is crucial. The policy should be reviewed periodically to ensure that it is 'fit for purpose'.

Communication of the policy is important to:

— demonstrate to stakeholders (e.g. employees, community) the commitment of top management and the organization to biorisk management;

— raise awareness of the commitments made in the policy statement;

— explain why the biorisk management system is established and is maintained; and

— guide individuals in understanding their biorisk responsibilities and accountabilities.

When communicating the policy to both new and established personnel, consideration should be given to creating and maintaining awareness on how biorisks are managed. The policy can be communicated in alternative forms to the policy statement itself, directly through induction and continuous professional development programmes, or indirectly through the use of wallet cards, posters, etc. In communicating the policy, account should be taken of issues such as diversity in the workplace, educational background, language skills, etc. It is for the organization to determine how it wishes to make the policy available to its stakeholders, e.g. through publication on a web site, or by providing printed copies on request.

4.3 Planning

4.3.1 Planning for hazard identification, risk assessment and risk control

4.3.1.1 Planning and resources

The organization shall ensure that a risk assessment system is established, implemented and maintained in accordance with this standard and that the performance of the risk management system is reported to senior management for review and as a basis for improvement.

The organization shall identify resource requirements and provide adequate resources, including the assignment of trained personnel for management, performance of work, and verification activities, including internal review.

The organization should continuously assess and mitigate risk. The organization should seek to understand the hazards and threats in and around the facility, the risk that they pose to employees and the surrounding community, and the impact they could have on operations.

Planning for hazard identification, risk assessment, and risk control should include understanding the external influences which may define the level of risk tolerance and risk control measures. These include but are not limited to:

— legal and other requirements;

— internal policy;

— management approval and appropriate resources; and

— qualification and training of personnel.

The roles and responsibilities of personnel who perform and verify work affecting biorisk management should be defined and documented, particularly for people who need the organizational freedom and authority to do one of the following:

a) initiate action to prevent or reduce the adverse effects of risk;

b) control further treatment of risks until the level of risk becomes acceptable;

c) identify and record any problems relating to the management of risks;

d) initiate, recommend, or provide solutions through designated channels; or

e) *communicate and consult internally and externally as appropriate*.

The organization's senior management or designate should have defined roles and responsibilities to be able to specify, implement and maintain a biorisk management system – including allocating adequate resources and assigning qualified staff – to ensure the continuous evaluation and mitigation of risks.

*There are many defined methodologies and approaches available for conducting risk assessments, and the approach taken will vary depending upon the nature of the situation and the level of detail required. One framework which organizations may consider adopting is outlined in Figure 1 below (*NOTE: this figure appears under section 4.3.1.2 in the CWA 15793:2008, but is included here to facilitate understanding of this section).

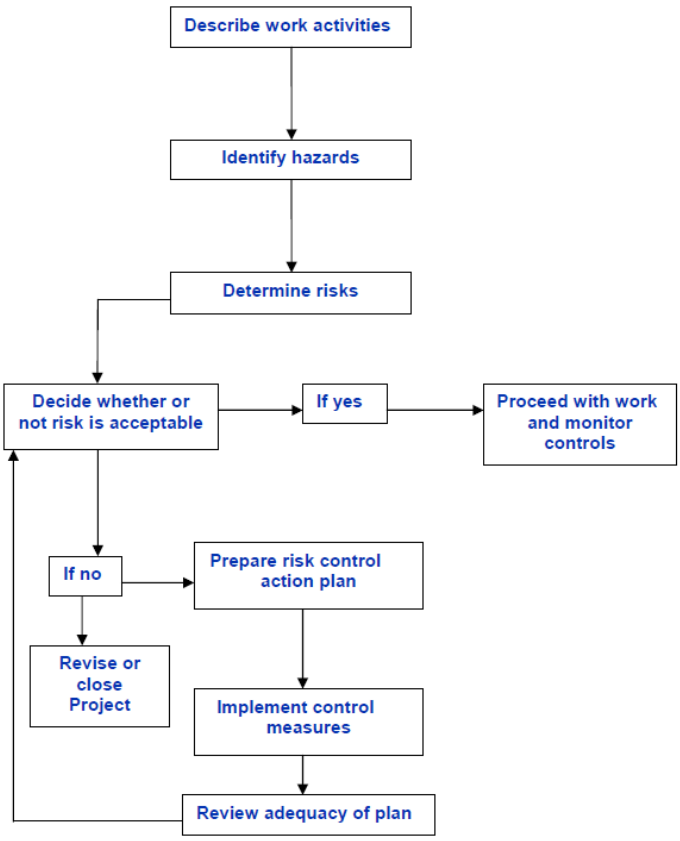

Figure 1 — Risk assessment strategy

4.3.1.2 Risk assessment timing and scope

The organization shall ensure the approach to risk assessment is defined with respect to its scope, nature and timing so that it is proactive rather than reactive.

Risk assessments should be carried out before new activities begin. Risk assessment also should be conducted whenever there is a change that affects the work environment, or in response to a laboratory incident. Risk assessments should be applied to all procedures and activities in the facility, including normal operations, periodic or rare laboratory procedures, and cleaning and maintenance.

The scope of the risk assessment should be focused on specific procedures and agents; multiple risk assessments may be required to adequately identify the risks and use the assessment to support risk control efforts.

Conducting risk assessments requires a comprehensive understanding of the organization's activities.

The following should trigger either a new risk assessment or review of an existing one:

a. *commencement of new work or changes to the programme of work, including the introduction of new biological agents or alterations to work flow or volume;*

b. *new construction / modifications to laboratories, plant and equipment or its operation;*

c. *introduction of altered* or *unplanned staffing arrangements (including contractors, visitors, and other non-core personnel);*

d. *significant alterations to Standard Operating Procedures (SOPs) or working practices (e.g. disinfection / waste management methodologies, Personal Protective Equipment (PPE) provision / usage entry / exit protocols, etc.);*

e. *when unexpected events that may have relevance for the management of biorisks are observed,* such as accidents, incidents (near misses) or changes in the security threat environment*;*

f. *when actual or potential non-conformity with internal / external rules and regulations is identified (e.g. introduction of new legislation or major accident exposure);*

g. *when considering emergency response and contingency planning requirements;* and

h. *as part of the existing management system review process (e.g. annually or at another appropriate and predetermined frequency).*

The scope, nature, and timing of the organization's risk assessments should be documented and be consistent with the initiation and completion of actual risk assessments.

4.3.1.3 Hazard identification

The hazards associated with proposed work shall be identified and documented.

The first stage in the biorisk management process is to identify all hazards and threats *that are relevant for biorisk. It is useful to involve the whole work team in this process and to use inputs from organizational experts on safety and biorisk management.*

A hazard may be a physical situation (e.g. a fire or explosion), an activity (e.g. pipetting), an external condition (e.g. weather, individuals who could steal and / or misuse materials or information*) or a material (in this case the principal hazard is most likely to be a biological agent or toxin, but others will include chemicals,* radiological materials *and asphyxiating gases such as nitrogen). The essence of a hazard is that it has the potential for causing harm, regardless of how likely or unlikely such an occurrence might be.*

Biological hazards and threats *should be identified and assessed in relation to their potential damage to humans, animals,* or *the environment* and requires knowledge of the facility, operational practices and experience of personnel. Generally, this identification process requires a multidisciplinary biorisk management team that relies on information and guidance from internal or external experts on safety, security, and biorisk management. Conducting a hazard identification exercise should also involve a review of legal and regulatory requirements, and a review of applicable guidelines and organization's codes of practice. This legal review will assist in identifying materials that are required by law, regulation, or guidance to be controlled within the facility. *Where hazardous materials are classified into hazard or risk groups based on international and / or foreign country classification schemes local diverging needs and constraints should be considered.*

A hazard identification exercise should use information including:

a) group experience and knowledge;

b) external or specialized expertise not found in the facility;

c) results of previous assessments;

d) surveys of previous accidents / incidents;

e) hazardous materials data;

f) information on hazardous organisms;

g) guidelines and codes of practice;

h) facility drawings;

i) SOPs, manuals, etc.;

j) process maps; and

k) results of task analysis*.*

Defined methodologies and approaches exist *for conducting hazard identification exercises. Unless hazards are identified effectively, it is not possible to assess the risk associated with the facility and associated activities. Hazard identification should be appropriate in nature, structure and recorded to a level whereby others can review the process.*

At the conclusion of the hazard identification process, the biorisk management team should have identified and documented the hazards and threats that apply to the specific facility's operations and be prepared to use this information in the subsequent risk assessment process.

4.3.1.4 Risk assessment

The organization shall ensure that suitable methodologies for assessing and recording risks are identified, implemented and maintained.

A repeatable, structured, analytical process should be identified and documented that can identify the risks to laboratory workers, the community, and the environment associated with identified hazards or threats. Periodic review of this methodology should be conducted, and the documentation should be updated accordingly.

The risk assessment should include, but should not be limited to the following elements:

— properties of organisms, including availability of treatment, vaccines, or prophylaxis;

— laboratory procedures, work structure, equipment, facilities (i.e.: biocontainment/biosafety level) and controls;

— personnel health status, qualifications, training, and human factors (e.g. behaviour, reliability, errors);

— environmental conditions, including endemic pathogens, and external threats; or

— legislation, rules, and requirements where appropriate.

The risk assessment should categorize and prioritise *risks to identify those which need to be eliminated or controlled*. Risk is a function of the likelihood and consequences of an adverse event. *Descriptions of likelihood and consequence, together with the acceptability of risk levels should be defined and used in the assessment.* Likelihood is the probability of an adverse event occurring. Consequence is the severity of the incident. Adverse events can include accidental exposure, loss, theft, misuse, or intentional unauthorized release of biological materials or related information. The likelihood and consequences of each potential adverse event should be evaluated, and the criteria used to define likelihood and consequences should be clear, consistent, and documented.

Risk *assessments can be* achieved using a *qualitative, semi-quantitative or quantitative* methodology. *A method suitable to the situation should be identified,* documented, and *followed*. *Such a classification can be achieved, for example, through the use of a risk matrix identifying likelihood and consequence categories, ordered to illustrate those falling into high, moderate and low zones. However, other approaches also may be relevant and appropriate.*

In conducting risk *assessments due considerations* should *be made* to carefully consider *the inherent risk from the biological agents and toxins (e.g.* from *risk grouping descriptions*, such as route of infection, host range, mortality and morbidity, treatment options to *material safety data sheets etc*.), as well as how that risk changes based on the way that the biological agents are used in the laboratory. Risk assessments should specifically analyze the unique experiment and protocols, equipment and controls, personnel, and laboratory environment where those agents will be used. The risk assessment also should include a threat assessment component. A threat assessment is the process of identifying and characterizing the specific threats to a facility or laboratory and to determine if and how a threat could cause harm.

The results of the assessments should be used to prioritise risks, evaluate the risk tolerance for the organization, and to determine what risk mitigation measures should be implemented to reduce risk to acceptable levels. *After definition and implementation of control measures, the risks should be reviewed to decide if the remaining risk is acceptable or whether additional controls need to be identified and implemented.*

4.3.1.5 Risk Management

The organization shall ensure suitable methodologies for the allocation of actions resulting from risk assessments, including time lines, responsible persons and associated reporting and approval mechanisms are identified, implemented and maintained.

Management should develop a strategy to determine the risks at the facility, and to implement the controls necessary to reduce the risks to acceptable levels. It is the responsibility of the management of the organization to ensure that the level of risk is acceptable.

Risk management may include, but is not limited to, the following:

— management commitment;

— results of the risk assessments;

— identification of institutional level of risk tolerance;

— results of internal and external monitoring and evaluations; and

— implementation of mitigating measures.

The risk management approach should include a control plan to include:

a) who is responsible and accountable for implementation of the plan;

b) what resources are to be utilized (e.g. people, budget);

c) timetable for implementation; and

d) details of the mechanism and frequency of review of compliance with the plan.

Risk mitigation *strategies should consider the "hierarchy of control"* as follows:

— *elimination of the work* producing the hazard always should be considered first. If the hazard cannot be eliminated completely, the next control measures may be applied to prevent or minimize exposure to the risk. It generally is a combination of these;

— *substitution with an alternative organism / activity.* It involves changing the agent or hazardous material, process, or equipment for one that is less hazardous. Reduction of quantity and / or frequency may also be an option;

— *use of engineering controls* for *isolation of the hazard* from the employee / staff or to secure materials;

— *administrative controls* include SOPs, training, supervision, and time limitations on the execution of the task for all staff who work within or support laboratory operations; and

— *reliance on personal protective equipment (PPE).* PPE should be used when the risk cannot be adequately controlled by a combination of the above methods. PPE should not be used as a substitute for engineering controls. Selection of PPE should be based on considerations in clause 4.4.4.5.4.

Specific control measures should be regularly tested and maintained to ensure continuous performance. In addition, the entire risk management process should be regularly monitored and reviewed to ensure that it

continues to achieve the goals of reducing risks to acceptable levels. Documentation should include the monitoring and review procedures of the entire risk management system, including the names of those responsible for these tasks.

The facility should have and execute an implementation plan for institutional risk assessment, mitigation, and review.

4.3.2 Conformity and compliance

The organization shall ensure that all relevant requirements are identified and fulfilled within the biorisk management system. Legal requirements include national / federal, regional / state, provincial, city and local regulatory requirements with which the organization has to comply.

The organization should adopt measures to identify legal and other requirements for the facility in relation to the biological agents and toxins that will be held and used, but also other regulations including, for example: worker protection and rights, environmental impact and general health & safety (e.g. fire, electrical, etc.).

Legal requirements can take many forms, such as:

— legislation, including statutes, regulations and codes of practice;

— decrees and directives;

— orders and “regulatory” guidelines issued by regulators;

— permits, licences or other forms of authorization;

— judgements of courts or administrative tribunals; and

— treaties, conventions, protocols.

Examples of other requirements can include:

— contractual conditions;

— agreements with employees;

— agreements with interested parties;

— agreements with health authorities;

— non-regulatory guidelines;

— voluntary principles, best practices or codes of practice, charters (e.g. National Sanitation Foundation Code No. 49, Biological Safety Cabinets); and

— public commitments of the organization or its parent organization, and corporate / company requirements.

Some of these commitments or agreements can address a range of issues in addition to biorisk matters. The biorisk management system need only address such commitments or agreements to the extent that they relate to the organization’s biorisks.

The organization may choose to appoint a responsible person to seek information on legal and other requirements and to ensure that relevant information is disseminated throughout the organization.

Depending on the nature of its biohazards, operations, equipment, materials, etc., an organization should seek out relevant applicable biorisk legislative or other requirements. This can be achieved through the use of knowledge within the organization and / or using external sources such as:

— the internet;

— libraries;

— biological safety professional associations and networks;

— trade associations;

— regulators;

— legal services;

— biorisk experts;

— equipment manufacturers;

— materials suppliers;

— contractors; and

— customers.

Having identified what is applicable, the organization's procedure needs to include information on how it can access the legal and other requirements. There is no requirement to maintain a library; it is sufficient that the organization be able to access the information when needed.

There is a need to monitor for new and upcoming requirements, as well as those already in existence. This information should be kept up to date and the requirements incorporated into the biorisk management system of the facility.

4.3.3 Objectives, targets, and programme

4.3.3.1 Biorisk control objectives and targets

The organization shall establish, implement and maintain documented biorisk control objectives and targets for an effective control of biorisk at relevant functions and levels in the organization.

Setting objectives is an integral part of the planning for a biorisk management system. An organization should set objectives to fulfil the aims of its biorisk policy, including its commitments to continually improve biosafety and biosecurity.

Organizational objectives related to biorisk management should be defined, documented and communicated to employees. These objectives should be prioritised based on the outcome of the risk assessments and should lead to agreed milestones to ensure measurable progress. These documented goals – along with measurable results – should be communicated to stakeholders as an assessment of the progress of the implemented biorisk programme.

The process of setting and reviewing objectives and implementing programmes to achieve them provides a mechanism for the organization to continually improve its biorisk management system and to improve its biorisk performance.

When setting biorisk objectives the organization needs to take account of legal and other requirements and the outcomes of the risk assessment. The organization should make use of the information obtained from the planning process to determine whether it needs to set specific objectives in relation to any of its legal and other requirements, or its biorisks.

The organization also should consider the incorporation of a number of factors such as:

— policy and objectives relevant to the organization's business as a whole;

— results of hazard identification, risk assessment and existing controls;

— evaluations of the effectiveness of the biorisk management system (e.g. from internal audits);

— metrics regarding the same activities being done at other organizations, to the extent metrics are available;

— technological options, financial, operational and business requirements;

— information from employee consultations, reviews and improvement activities in the workplace (these activities can be either active or reactive in nature);

— analysis of performance against previously established biorisk objectives;

— past records of biorisk nonconformities and incidents;

— the results of the management review; and

— the need for and availability of resources.

Objectives should be developed which are clear, precise, well-defined and understandable. They should provide clear criteria which can be used to confirm if the objective has been accomplished. The objective should be achievable and realistic. The objectives should also have clear timelines and milestones.

A common concept used to summarize this process is also known as SMART: Specific, Measurable, Achievable, Realistic, Timely.

It is also advisable that the organization records the background and reasons for setting the objectives in order to facilitate their future review. Objectives are sometimes given associated "targets". For the purpose of the CWA 15793:2008, "targets" are viewed as being a sub-set of objectives.

Examples of types of objectives can include those that:

— increase or reduce something that specifies a numerical figure (e.g. increase to 50 % the number of workers that have undertaken a biosafety refresher training course);

— introduce controls or eliminate hazards (e.g. to remove all unnecessary glassware from BSL3 laboratories);

— substitute biological agents of a lower risk for specific activities;

— increase worker satisfaction in relation to biorisk (e.g. for a reduction of workplace stress);

— reduce the number, volumes or location of biological agents stored at the facility;

— reduce the access to biological agents, equipment or processes (e.g. the introduction of access controls);

— increase awareness or competence in performing work tasks securely or safely; and

— meet impending legal requirements prior to their enactment.

Specific biorisk objectives or targets can be established by different functions and at different levels within the organization. Certain biorisk objectives, applicable to the organization as a whole, can be established by top management. Other biorisk objectives can be established by, or for, relevant individual departments or functions. Not all functions and departments are required to have specific biorisk objectives.

In order to achieve the objectives, a programme of action should be established. For complex issues and for higher risk activities, more formal project plans may also need to be developed as part of the programme(s). In considering the means necessary to establish the programme(s), the organization should examine the resources required (financial, human, infrastructure) and the tasks to be performed. Depending on the complexity of the programme the organization should assign responsibility, authority, and completion dates for individual tasks to ensure that the biorisk objective can be accomplished within the overall timeframe. The biorisk objectives and programme(s) should be communicated (e.g. via training and / or group briefing sessions, etc.) to all relevant personnel. Regular reviews of the programme(s) should be conducted and the programme(s) modified where necessary.

4.3.3.2 Monitoring controls

Management shall establish the controls and put in place documented procedures for monitoring the effectiveness of the controls being applied to reduce or eliminate the hazards identified in the risk assessment process.

Management cannot assume that effective controls identified during risk assessment are necessarily in place or will be put in place. *The controls can be monitored by regular audits, by utilizing corrective action reporting processes where problems have been identified, by investigation of incidents and accidents and improving controls and their implementation and by ensuring that adequate resources are provided to maintain the effectiveness of the controls*.

4.4 Implementation and operation

4.4.1 Roles, responsibilities and authorities

4.4.1.1 Top management

Top management shall take ultimate responsibility for the organization's biorisk management system.

Top management shall ensure that roles, responsibilities and authorities related to biorisk management are defined, documented and communicated to those who manage, perform and verify work associated with the control of biological agents and toxins.

Top management shall demonstrate its commitment by ensuring the availability of resources to establish, implement, maintain and improve the biorisk management system.

This standard has identified roles that need to be covered in the organization and has only used titles to illustrate these roles; these titles may not be the same as the titles used in specific organizations.

Top management includes Officers (Director General, Chief Executive Officer, Chief Operating Officer, Chief Financial Officer, etc.) and Directors of the organization. Overall responsibility for management of biorisk rests with top management but tasks may be delegated through the organization provided that they are passed to competent individuals with adequate resources to perform the activities safely and securely. In smaller organizations, one individual may hold more than one role described in the standard. It is important to define roles and responsibilities and that there is clear communication within the organization in terms of the actions that need to be taken, and who has the required authority.

The successful implementation of a biorisk management system calls for a commitment from all persons working under the control of the organization. This commitment should begin at the highest levels of management.

Top management should:

— determine and make available, in a timely and efficient manner the resources needed to prevent injuries and illness related to exposure to biological materials in the workplace;

— assign roles and ensure that everyone is aware of their responsibilities and level of accountability. When assigning roles, authorizations and responsibilities, potential conflicts of interest should be considered;

— ensure that those members of the organization's management with biorisk responsibilities have the necessary authority to fulfill their roles;

— ensure there is clarity of responsibilities at the interfaces between different functions (e.g. departmental, levels of management, workers, the organization and contractors, the organization and the community); and

— appoint one of its members as the person responsible for the biorisk system and reporting on its performance.

When determining the resources needed to establish, implement and maintain the biorisk system, an organization should consider:

— the financial, human and other resources specific to its operations;

— the nature and volume of biological agents stored or handled;

— technologies specific to its operations;

— the security / biosecurity threats faced by the organization;

— infrastructure and equipment information systems; and

— the need for expertise and training.

Resources include human resources and specialized skills, organizational infrastructure, technology and financial resources. Resources and their allocation should be periodically reviewed by management to ensure they are sufficient to carry out the biorisk programmes and activities, including performance measurement and monitoring. For organizations with established biorisk management systems, the adequacy of resources can be at least partially evaluated by comparing the planned achievement of biorisk objectives with actual results. In evaluating adequacy of resources, consideration should also be given to planned changes and / or new projects or operations.

CWA 15793:2008 requires that the responsibilities and authority of all persons who perform duties that are part of the biorisk management system to be documented. These can be described and included in:

— biorisk management system procedures;

— operational procedures or work station procedures;

— project and / or task descriptions;

— job descriptions;

— induction training packages.

In assigning roles and responsibilities, potential conflicts of interest should be considered.

4.4.1.2 Senior management

A senior manager shall be designated with operational responsibility for overseeing the system for management of biorisk.

Functions of the system for the management of biorisk shall include:

a) providing appropriate resources to ensure adequate provision of personnel, facilities and other resources deemed necessary for the safe and secure operation of the facility;

b) reporting to top management on the performance of the biorisk management system and any need for improvement;

c) ensuring promotion of the biorisk management system throughout the organization;

d) instituting review, audit and reporting measures to provide assurance that the requirements of this standard are being implemented and maintained effectively.

Senior managers are those with significant operational, budgetary and personnel authority at the departmental or higher level, and may include members of top management. The senior management representative should be an individual with decision-making authority at a level whereby he / she can allocate resources and make decisions regarding the biorisk management needs of the facility (including required resources to conduct risk assessments and other management and administrative activities) independently of the need to implement the programme of work.

4.4.1.3 Biorisk management committee

A biorisk management committee shall be constituted to act as an independent review group for biorisk issues. Reporting to senior management, the committee shall:

a) have documented terms of reference;

b) include a representative cross-section of expertise, appropriate to the nature and scale of the activities undertaken;

c) ensure issues addressed are formally recorded, actions allocated, tracked and closed out effectively;

d) be chaired by a senior individual;

e) meet at a defined and appropriate frequency, and when otherwise required.

The biorisk management committee is often recognized as the Institutional Biosafety Committee and may be either a dedicated function, or the role can be addressed through a committee with a wider remit (broader scope)*. Members may include the scientific manager, additional scientific specialists, the biorisk management advisor(s), security manager and the occupational health professional. Dependent on the nature of the agenda or nature of the work others may be included, e.g. the facility manager and / or worker and community representatives.*

Functions of the committee should include:

a) contributing to the development or updating of institutional biorisk policies and codes of practice;

b) approving proposals for new work or significant modifications to the potential risk associated with existing activities;

c) reviewing and approving protocols and risk assessments for work involving biological agents and toxins;

d) *reviewing information relating to significant accidents / incidents, data trends, associated local / organizational actions and associated communication needs*; and

e) providing and/or review of reports to senior or executive management regarding the status of the organization's biorisk program.

The list of roles for the biorisk management committee is neither exhaustive nor comprehensive, but includes some of the main areas that should be addressed.

4.4.1.4 Biorisk management advisor

A competent individual(s) shall be designated to provide advice and guidance on biorisk management issues. This individual shall report directly to the responsible senior manager and have delegated authority to stop work in the event that it is considered necessary to do so. This role shall be independent of those responsible for implementing the programme of work.

The competent individual providing advice and guidance on biorisk management is often recognized as a biological safety officer (BSO), biological safety advisor, or biorisk manager. This individual is to be appointed by executive management to manage the biorisk management program and is to report to a senior manager

in the organization. *This function normally should be regarded as an advisory position and not directly responsible for managing biorisk, as this rests with those conducting and managing the work within the organization (e.g. scientific director, principal investigator, department head, laboratory manager, group leader, etc). The role and knowledge of the biorisk advisor is important to develop, implement, maintain and continually improve a biosafety and biosecurity programme based on a management system. The advisor should be competent to perform the role, and allocated sufficient time and other resources to do the job effectively.* Organizations may use international references on biosafety professional competence (e.g. CWA 16335:2011) or national standards on biosafety professional competence of value when seeking to designate a biorisk management advisor. *In the execution of his / her biorisk management duties the advisor should be independent from those responsible for implementing the programme of work and have direct access to the top management representative when necessary.*

Functions of the biorisk management advisor should include:

- developing policies and procedures, or sections thereof, that pertain to biosafety activities, i.e., safety equipment usage.

- *verifying, in conjunction with other relevant personnel, that all relevant biorisk considerations have been addressed;*

- *advising or participating in the reporting, investigation and follow-up of accidents / incidents, and where appropriate referring these to management / biorisk management committee;*

- *ensuring that relevant and up-to-date information and advice on biorisk management is made available to scientific and other personnel as necessary;*

- *advising on biorisk management issues within the organization (e.g. management, biorisk management committee, occupational health department, security);*

- *contributing to the development and / or delivery of biorisk training activities*; and

- *ensuring that all relevant activities are performed in compliance with biorisk regulations and that required biorisk authorizations for work are in place.*

The list of roles for the biorisk management advisor is neither exhaustive nor comprehensive, but includes some of the main areas that should be addressed.

4.4.1.5 Scientific management

An individual(s) with responsibility for the scientific programme within the facility shall be designated with responsibilities relevant to biorisk management.

Functions shall include:

a) ensuring that all work is conducted in accordance with established policies and guidelines described in this standard;

b) supervising workers, including ensuring only competent and authorized personnel can enter and work in the facility;

c) planning and conducting work activities, and ensuring adequate staffing levels, time, space and equipment are available;

d) ensuring required authorizations for work are in place;

e) ensuring laboratory biosafety and laboratory biosecurity risk assessments have been performed, reviewed and approved, and that the required control measures are in place;

f) ensuring that all at-risk employees have been informed of risk assessments and/or provisions for any recommended precautionary medical practices (e.g. vaccinations or serum collections).

The scientific manager is the individual responsible for managing the scientific programme within the facility on a day-to-day basis, and for implementing and monitoring biorisk controls in association with other facility personnel (e.g. adherence to policies and procedures, monitoring staff performance and participation in inspections and audits). The individual would normally have an in-depth knowledge of the work programme and the facility and be in a supervisory / management position and may be referred to as Head of Department, Principal Investigator, Laboratory Supervisor / Manager or Group Leader. Competence will be required in technical / scientific aspects of the biological agents and toxins being used and their control, together with management of the facility, its personnel and systems. More than one individual may hold similar roles, but in such instances the responsibilities should be clearly defined so as to avoid any omissions and ensure consistency.

Managers should provide visible demonstration of their commitment to continual improvement of biorisk performance. Means of demonstration can include visiting and inspecting sites, participating in incident investigation, and providing resources in the context of corrective action, attendance and active involvement at biorisk and safety meetings, communicating the status of safety activities, and acknowledging good biorisk performance.

It is possible that a scientific programme might include field work, and even if it occurs outside a facility, it is the responsibility of the scientific manager to ensure that appropriate biorisk procedures are implemented and monitored as part of the biorisk management system.

4.4.1.6 Occupational Health

The organization shall have access to appropriate occupational health expertise and establish an occupational health programme commensurate with the activities and risks of the facility.

The occupational health programme should encompass the worker health programme (4.4.4.6). *The occupational health professional would normally be a medical doctor or occupational health nurse with understanding of the biological agents and toxins that are handled within the facility.*

The role should include:

— *providing input into* work practices *from a worker health perspective;*

— *providing input into risk assessments from a worker health perspective;*

— *advising on first aid / emergency treatment measures and follow-up*;

— *liaising with external healthcare providers*;

— *coordinating medical examinations, surveillance and vaccination programmes* (4.4.4.6.1);

— advising on appropriate PPE in collaboration with the management biorisk advisor; and

— developing pre- and post-exposure protocols.

Roles and responsibilities of the occupational health professional should be determined in light of requirements set out in this standard.

4.4.1.7 Facility management

Facilities manager(s) shall be appointed with responsibilities relevant to facilities and equipment determined in accordance with requirements set out in this standard.

The facilities manager normally would be an engineer or someone with an in-depth knowledge of laboratory facilities, containment equipment and buildings. The role should include providing input into risk assessment from a facility perspective, coordinating building and maintenance work, and liaising with contractors. Roles and responsibilities of the facilities management personnel should be determined in light of requirements set out in this standard. More than one individual may hold similar roles, but in such instances the responsibilities should be clearly defined to avoid any omissions and ensure consistency.

4.4.1.8 Security management

A security manager shall be designated with responsibilities determined in accordance with requirements set out in this standard.

The organization should designate an experienced individual *with an in-depth knowledge of laboratory and facility security* to manage and coordinate a comprehensive security programme. The security manager can be a member of the Biorisk Management Committee. The security manager *should liaise with* laboratory *personnel* and other management, and *implement effective and proportionate laboratory biosecurity measures, based on the biological risk* assessments and management priorities. The security manager should contribute to facility *risk assessments and* biorisk management *from the security perspective. Roles and responsibilities of the security personnel should be determined* in accordance with the *requirements* established by CWA 15793:2008.

The security manager should be appointed by the organization's management, based on security needs of the institution and should report to executive management. This position should have clearly defined roles and responsibilities with adequate resources for the security manager to carry out his or her job functions and requirements. The chain of command and where the security manager fits in the organizational structure should be clear.

The security manager should, in close consultation with the biorisk advisor and the Biorisk Management Committee, plan, document, and implement the risk mitigation measures for all the different aspects of security at the facility. The security manager should be responsible for the facility security plan, which should include: transport security, information security, personnel security, physical security, and material control and accountability. The security manager should implement and document a regular review and performance test of all of the procedures, equipment, and personnel associated with the operation of the security system. A multidisciplinary team should review the written security plan and should conduct security exercises periodically to test the facility security system.

The security manager should ensure that the facility has a comprehensive security system, including appropriate staffing, systems, and procedures. The security plan should be the responsibility of the security manager, who should be a competent individual with the authority and responsibility to address security risks and threats at the facility.

4.4.1.9 Animal handling

In laboratories where animals are maintained, an animal care manager shall be designated with responsibilities determined in accordance with requirements set out in this standard.

The organization should designate an individual who is responsible for animal-related aspects of the biorisk programme in the facility. This individual should have expertise in the use of laboratory animals and safety with animals. He or she should ensure that animals are handled in a safe and secure manner that prevents potential transmission of biological agents from animals to humans and their unintended release into the environment.

The animal care manager normally would be someone with an in-depth knowledge of animal handling, care and ethics, including related technical equipment and apparatus, as well as animal welfare and husbandry, *zoonotic and animal diseases* with their associated occupational health issues*. The animal care manager should liaise with other personnel (e.g. biorisk management advisor, occupational health professional*, *etc.) to implement effective and proportionate laboratory biosafety and laboratory biosecurity measures. A qualified veterinarian should be available for additional advice. The role should include providing input into risk assessment and management* systems *from an animal care and use perspective.*

According to the animal species present in the facility, he or she should determine what risks they pose and implement risk-based mitigation strategies, such as:

a) using HEPA filtered animal caging when appropriate;

b) using BSC or other containment devices whenever needed;

c) wearing of personal protection appropriate for species and work being undertaken;

d) evaluating the appropriateness of the training and experience of the individuals working with animals;

e) assessing the appropriateness of the animal facility; and

f) using appropriate procedures / techniques to eliminate accidents in connection with care and manipulation of laboratory animals.

The result is the provision of a facility that works safely and securely with animals by taking all reasonable risk mitigation measures and, in addition, conforms to animal husbandry requirements, preventing injuries and exposure to biological agents.

4.4.2 Personnel training, awareness and competence

The organization shall ensure that personnel that have responsibilities and/or perform tasks that may impact biorisk management in the workplace are competent to do so. Competence levels shall be judged on appropriate education, training and experience.

The organization shall define required competency levels and shall maintain records verifying that staff members have attained and demonstrated those levels of competency.

The organization should have a comprehensive proficiency programme in biorisk management The training should ensure that personnel are fully informed and are able to implement the skills and ideas deemed important by the organization.

Organizations should have effective procedures for ensuring the competence of personnel to carry out their designated functions through having defined training programmes. The organization should also assess the ability of people to perform their work competently. The organization should define how they would assess their employees competency and authorization level to perform their work. The organization should detail how their training programmes are organized, monitored and evaluated. The organization should define the different types of training they will require for different types of work.

Training examples may include:

— biorisk policies and objectives;

— definition of roles and responsibilities;

— procedures and operating instructions for training;

— training and relevant continuous professional development programmes required;

— competent personnel for “train the trainer” and mentoring programmes;

— hazard identification, risk assessment and risk mitigation results; and

— employee performance evaluation.

The organization should define and record responsibilities and associated competency levels that impact on biorisk management as part of a comprehensive staff ‘Continuous Professional Development Programme’.

Training Programmes should equip staff with the knowledge and tools to identify hazards, manage risk, and put into place measurable markers of success that can be reported to and used by management.

4.4.2.1 Recruitment

The organization shall ensure that qualifications, experience and aptitudes relating to biorisk are considered as part of the recruitment process.

The organization should hire technically capable, biorisk conscious, reliable staff members to contribute to the mission of the organization and reduce its risk through their safe and secure work practices.

Factors that can be considered during recruitment are:

— technical competence and relevant experience;

— health conditions that may put the potential employee at risk in the laboratory;

— reliability;

— integrity; and

— willingness to comply with laboratory SOPs and procedures.

Prior to employing someone*, the organization should ensure that*:

a) all personnel should be subject to a formal selection process, including relevant background checks, based on risk (e.g. employment references, security checks, etc.);

b) appropriate checks *are implemented if existing employees are transferred to areas where there may be a* different *risk profile;* and

c) an assessment is made of the need for the above controls for non-core personnel (e.g. contractors, visitors, students, etc.), and measures implemented to ensure they are applied where necessary.

d) procedures that include biorisk understanding and implementation should be developed for recruitment and personnel management.

Local laws should be considered to avoid discriminatory recruitment practices.

The result should be a professionally competent, safe, secure, and productive workforce that promotes the success of the organization.

4.4.2.2 Competence

The organization shall ensure that personnel conduct activities within the facility under close supervision until competency has been demonstrated.

The organization should put monitoring systems in place to ensure that personnel are competent to perform their tasks safely and securely. Supervision is appropriate for all new, inexperienced, or visiting personnel or workers who have not demonstrated full competence in their new working environment. All personnel should be re-assessed periodically for competence on a timetable determined by the organization.

Competence is defined in relation to appropriate education, training and / or experience, together with a demonstrable ability to perform the task in a safe and secure manner.

Procedures should address:

— *definition of competency needs;*

— *demonstration of successful completion of required training by competent trainer;*

— *demonstration of ability to perform tasks under supervision and unsupervised;*

— *restrictions on personnel who have not demonstrated full competence to ensure they do not perform tasks for which they are not* qualified and / or approved; and

— *maintenance of adequate training records.*

No worker should be exempt from demonstrating competence irrespective of rank, experience, or background, including management.

The organization should ensure that staff takes initial and periodic training to ensure safe and secure performance of tasks. Management should monitor and assess biorisk competency regularly and consistently in a measurable way that can be demonstrated to external agencies.

4.4.2.3 Continuity and succession planning

The organization shall ensure that adequate back-up and contingency measures are in place to address the need for continuity and succession planning.

The organization should identify roles and individuals and ensure that the integrity of the facility is not compromised through short or long-term absence. Such measures should include succession planning for personnel (technical, management and scientific, including contractors) to ensure that no individual holds critical knowledge regarding the safe and secure operation of the facility that is not available to others in the event of their departure or unavailability.

The organization should integrate continuity succession planning into the business continuation strategy of the organization.

The result is a robust organization that is not left with gaps in their knowledge and capability to continue working safely and securely when an individual leaves expectedly or unexpectedly.

4.4.2.4 Training

The organization shall ensure that requirements and procedures for biorisk-related training of personnel are identified, established and maintained.

The organization should design, establish, maintain, assess and monitor a robust biorisk-related training programme appropriate to all levels of personnel. The training should include raising personnel awareness of biorisk issues including the relevance of human factors (e.g. behaviour, reliability, errors) in biorisk management.

The result should be a training programme that provides staff with the knowledge and skills to reduce risk, with measurable markers of success that can be reported to management.

In order to design a training programme the organization should consider - apart from the ones already given:

— *definition of* employees duties and their *training needs* related to *biorisk* (e.g. analysis of employees past performance);

— biorisk policies and objectives;

— safety and security competencies that are required at different levels of the organization;

— *provision of required biorisk training;*

— frequency of training;

— awareness programmes for contractors, temporary workers and visitors;

— *determination of effectives of biorisk training*;

— choice of the appropriate method for conducting the training (e.g. web based, instructor led, hands-on training);

— *restrictions on personnel to ensure they do not perform tasks for which they are not trained;* and

— documentation and *maintenance of adequate records* of training that include attendance and content of training.

Training programmes should equip staff with the knowledge and tools to identify hazards, manage risk and put into place measurable markers of success that can be reported to and used by management.

4.4.3 Consultation and communication

The organization shall ensure that relevant biorisk information relating to its activities is communicated to and from employees and other relevant parties.

Employee involvement and consultation arrangements shall be documented.

Personnel shall have access to adequate and up-to-date information pertaining to the biorisks of the organization.

Successful biorisk management depends upon clear, concise and timely communication. This includes both internal (e.g. employees) and external (e.g. regulatory agencies, community representatives) communication.

Typical examples of communication may include:

— policy and objectives;

— employee consultations;

— public or community based meetings;

— review of activities in the workplace (both proactive and reactive);

— training programmes; and

— signage (e.g. labels, postings, notices).

The organization should implement mechanisms to ensure that relevant and current information with the potential to affect workers and others is defined and delivered effectively at appropriate intervals. In the workplace this could mean regular team meetings and briefings, as well as formal training sessions. In addition to facility personnel, it also may be appropriate to engage others, including:

a) local, national and international governmental organizations;

b) relevant regulatory agencies;

c) certifiers;

d) emergency services and healthcare providers;

e) contractors and suppliers (e.g. cleaners, maintenance providers, security personnel); and

f) local community representatives (e.g. through a community liaison committee).

Systems should be set in place to identify existing or emerging technologies or other relevant information relating to the containment of the biological agents and toxins being handled or stored, and to ensure that *this information is shared with relevant staff through the use of appropriate media. This may include circulation of appropriate signage, documents, team briefings and maintenance of reference libraries and other sources of information.*

A proactive communication and consultation process (e.g. committees, open forums, written communiqués) should be used to encourage participation in good biorisk reduction practices, and support of biorisk policies and objectives, from all those affected by the facility's operations.

These consultations should include employee involvement in identifying hazards, risk assessment, development of biorisk objectives, and risk mitigation strategies. The biorisk manager or team should meet with employees to discuss these topics and solicit suggestions. The frequency of the communications should be developed based on the needs of both internal (e.g. employee) and external (e.g. community) stakeholders to be informed of the issues.

The typical outcome is a communication programme which effectively provides information on biological risk and biosafety to all impacted and interested groups.

4.4.4 Operational control

The organization shall identify those operations and activities that are associated with possible biological risk and where control measures shall be applied.

The organization shall plan these activities, including maintenance, and ensure that they are carried out under specified conditions.

The organization should establish and maintain a comprehensive operational programme to ensure the effective application of biological risk evaluation, control and mitigation. Within that operational programme, the organization should establish procedures to control and mitigate biorisks based on biorisk management policy and objectives, risk assessment results, and legal requirements. These procedures should address laboratory operations, as well as other related biorisk issues, such as material transportation, inventory records, storage, and control systems. The organization should integrate these controls with those related to purchasing goods, equipment and services; entry of and access by contractors and other visitors; testing and maintenance of the equipment; and, the overall biorisk management system. Documented procedures should exist for those other situations where their absence could lead to deviations from the biorisk management policies and objectives.

These procedures should be reviewed on a regular basis for suitability and effectiveness. Changes to these procedures should be made whenever necessary.

4.4.4.1 General safety

The organization shall ensure that a formal process is in place to identify and manage risk associated with general safety.

The organization should adopt a preventive and proactive approach to managing such sources of risk, both to protect workers from the direct hazards associated with their work and to address the implications for biorisk in the event of an accident / incident resulting from such sources. Measures should be identified and implemented to detect, mitigate and respond to emergencies, taking into consideration the potential implications for the control of biological agents and toxins.

Issues addressed should include but are not limited to:

a) general laboratory safety;

b) fire safety;

c) electrical safety;

d) radiation safety;

e) chemical safety;

f) use of gasses (including risk of asphyxiation);

g) hot work and cold work;

h) equipment under pressure;

i) laboratory animal care and use;

j) general housekeeping, including storage requirements and tidiness; and

k) environmental safety.

The result should be that the biorisk management system includes references and links to the management systems related to the other risk present in the work place, so that the personnel know the measures applied for the other risks and have a global point of view about safety and security in the workplace.

4.4.4.2 Biological agents and toxin inventory and information

The organization shall ensure that an accurate and up-to-date biological agents and toxin inventory is established and maintained.

It shall ensure that records relating to the inventory of biological agents and toxins are current, complete and stored securely with adequate backup provision.

It shall ensure that transfers of biological agents and toxins between laboratories at the facility or into and out of the facility are recorded and controlled in line with the level of the risk.

The organization shall keep an accurate inventory of all biological agents and toxins that are stored and / or currently in use. The inventory should list and identify the specific person using the material, how and what it is being used for (including amount) and the location of its use and storage. The inventory process should be based on risk. The organization should develop systems of work that document authorized access and audit control mechanisms. All biological agents should be assigned to a designated and trained individual (i.e. researcher) to maintain an up-to-date inventory to avoid orphaned cultures.

The system should be set up for easy access for audit / control by authorized individuals and management. Access to the inventory should be limited to those individuals whose work requires access to that information.

Element of an inventory may include:

- a list of *all biological agents and toxins held, including cultures, specimens and other sources (e.g. seed stocks, working stocks, infected tissues / samples or animals*, recombinant material). The list should include:
  - the rationale for storing or keeping the agent or toxin;
  - the level of control in a specified location, including the possibility to *indicate legible and robust identifiers;*
  - *records of quantities and volumes at an appropriate level and based on risk; and*
  - *segregation and storage of biological agents and toxins according to risk.*
- a list of all projects using relevant biological materials (e.g. infectious, genetically modified); the risk assessments performed for them, the level of control, the permits obtained (if applicable) and their status (active / terminated) in specific locations;
- *the name(s) of and contact information for the individual(s) responsible for the material and details of other personnel with access to the materials or immediate area based on the level of the risk;*
- identification and *implementation of effective physical security measures according to risk (e.g. locks, alarms, access controls, etc.)* in a specific location;
- *development and maintenance of a reliable sample identification system;*

— identification of personnel *with a demonstrable, legitimate need* to access to the system, *biological agents* or *toxins*;

— determination of conditions for transportation of biological materials (shipment tracking, verification, responsible personnel); and

— *an inventory of* biological *materials* sent and received, including *materials consumed, destroyed or removed from the facility where appropriate.*

Controls should be set in place to ensure that all the necessary checks and documented assurances are received to ensure that requests for biological agents and toxins originate from legitimate facilities and individuals. Material only may be brought into the facility or sent elsewhere if authorized by those responsible for the facility. For materials deemed high risk, more stringent controls including shipment tracking and verification of receipt are important considerations.

The result could be the following;

— an inventory of biological material; documentation and regulations describing conditions for handling, transfer of biological materials with an appropriate level of risk;

— a list with contact information of responsible personnel with the access to biological materials; and

— *record of materials* sent, received *consumed, destroyed, or removed* that is controlled in line with the level *of risk.*

4.4.4.3 Work programme, planning and capacity

The organization shall ensure that the programme of work for the facility is defined, documented and reviewed.

The organization shall establish criteria for work that requires prior approval.

It shall ensure there is sufficient resource capacity and capability to manage workflow, whether planned or unplanned.

The objective is for the organization to ensure that the facility is appropriate for the work to be conducted.

Elements of a programme may include:

— the scope and extent of the work to be conducted;

— hazards identified;

— processes and procedures to be performed;

— results of workplace health risk assessments;

— number and type of personnel required for the scope of the procedures and processes to be conducted;

— working with proper leadership and decision makers to ensure *the resources needed to implement and maintain the biorisk management system and continually improve its effectiveness should be determined and provided;*

The organization should plan and document the programme of work in the facility, roles and responsibilities for the employees, and the approval requirement, as part of its planning and capacity measurement process. Actions required for this purpose may include:

— documenting a programme of work for the facility addressing the defined scope, roles, resources, and agents / toxins in use; and

— periodically review the scope of the work to assess for any changes needed.

The programme of work should include the nature of the activities authorized to be conducted in the facility and their definitions (e.g. diagnostics, research, small scale / large scale, etc.). All activities associated with the work programme should be specified and supported by formal SOPs approved in accordance with the requirements for controlled documents as defined by this standard. Any changes to the programme of work should be subject to a formal change management process.

The effect should be that the work at the facility is appropriately planned and adequately resourced (for facility, financially and staffing) before being undertaken.

4.4.4.4 Change management

The organization shall ensure that all changes associated with the design, operation and maintenance of the facility are subject to a defined and documented change management process.

Management of change is the continued review of the operations and the adequacy of the personnel and facilities for the scope of the operations. Roles and responsibilities of all those involved should be defined, and all relevant documents should be reviewed, verified and validated on a regular basis.

All changes should be communicated to all relevant persons.

The organization should have a process for systematically identifying and documenting any changes associated with the design, operation and maintenance and for modifying its biorisk management before changes are implemented.

The changes should be reviewed, verified and validated as appropriate, and approved before implementation. This should include evaluation of the effect of the changes on the risk assessment. Any change should trigger a renewed risk assessment of the project, workstation, or facility.

The following are examples of changes that should be subject to the change management process:

a) modifications to buildings and equipment or their operation, which may or would have an effect on biorisk;

b) introduction of altered staffing arrangements (such as temporary presence of on-site contractors or students, temporary reassignments of personnel);

c) changes to the programme of work, including alterations to work flow or volume which may or would have an effect on biorisk;

d) alterations to SOPs, including significant changes in materials or reagents;

e) modifications to entry / exit protocols;

f) modifications to personnel policies and visitor protocols;

g) modifications to disinfection and other waste management methodologies;

h) changes associated with PPE provision and usage

i) feedback from employees regarding problems with current operations, facilities or practices that were not included in the risk assessment;

j) feedback from incidents (near misses) and accidents; and

k) communication on external factors which may impact biorisk management, e.g. suppliers, equipment manufacturers.

As a result the organization will have in place a systematic process to address change, eliminating the potential for unintended events resulting for the lack of planning and unanticipated changes.

4.4.4.5 Work Practices, decontamination and personnel protection

4.4.4.5.1 Good microbiological technique

The organization shall ensure that all personnel handling biological agents and toxins are competent in good microbiological techniques and that appropriate resources (including time and equipment) are available to ensure such practices can be adhered to effectively.

The organization should ensure training and mentoring programmes that emphasize good microbiological technique to perform tasks safely and securely. The organization should have monitoring procedures to ensure that employees are competent to perform all tasks using good microbiological practices that are suitably supervised.

The organization should establish procedures to:

— set a standard for good microbiological technique and document it;

— train to this standard, promote it through the organization's communication process;

— use monitoring controls to assure people maintain the standard;

— allocate resources;

— assess personnel, product, environmental contamination following the laboratory procedures if warranted from either a biorisk or quality control perspective; and

— *as appropriate, procedures should address risks associated with but not limited to the following:*

a) animal handling;

b) centrifugation;

c) control of needles and sharps;

d) correct use of vacuum pumps;

e) culture, purification and storage techniques;

f) minimization / containment of aerosols;

g) pipetting;

h) sonication and other mechanical forms of cell / tissue disruption;

i) use of biological safety cabinets;

j) use of disinfectants, including spill control, routine decontamination, hand washing and showering; and

k) properly manage biowaste generated

This list is neither exhaustive nor comprehensive and identifies only some activities that may be employed during typical laboratory work. These activities should be undertaken in association with appropriate procedures and working practices to ensure the control measures are effective under all foreseeable and credible operating scenarios. Appropriate control measures should be identified during risk assessments, which will vary depending on the biological agents and toxins being used and the activities to be undertaken.

The output is a workforce that performs tasks safely and securely.

4.4.4.5.2 Inactivation of biological agents and toxins

The organization shall establish and maintain procedures to ensure that appropriate methods for disinfection and decontamination are chosen and implemented effectively.

The organization shall ensure that all contaminated or potentially contaminated waste items have been identified and documented (including those that may result from an emergency), and that effective procedures are put in place to devise effective decontamination and other appropriate treatments.

To inactivate biological agents and toxins handled in the facilities as safe and free of infectivity / toxicity to ensure the laboratory facility, personnel and equipment are safe and to ensure no biorisks are present in materials removed from the facility that could be the source of an unintended release into the environment.

Sources of contamination that should be considered include:

a) personnel;

b) clothing and PPE;

c) glassware;

d) equipment;

e) cultures and associated materials;

f) spill clean-up materials and equipment;

g) possibly infectious microorganisms and toxins and contaminated materials;

h) paper and plastic waste;

i) needles, syringes and sharps;

j) waste water, including that from sinks and showers;

k) air;

l) filters and air handling systems;

m) discarded equipment used in the facility;

n) animals exposed to laboratory biological agents or toxins;

o) animal carcasses and bedding; and

p) facilities.

Contaminated personnel may include core personnel working within the facility, contractors and emergency response personnel. Cultures and associated materials may be a source of contaminated supernatants, aspirates and culture media. Infected biological materials also may include infectious human, animal or plant specimens. In some instances it may be necessary to hold contaminated dedicated equipment such as fire fighter apparel or ambulance tools on site if they cannot be effectively decontaminated.

Whatever the biological agents and toxins handled, it is likely that a number of effective inactivation methods will be available. The organization should ensure that there are data available to demonstrate that the methodology selected is capable of inactivating the biological agents and toxins under the specific conditions encountered in the facility. Validation measures should consider issues including:

— *the nature of the material being treated (e.g. volume, presence of protein / other potentially inhibitory substances);*

— *contact times, materials compatibility issues (e.g. interaction with stainless steel or rubber seals);*

— *potential health hazards associated with the disinfectant;* or physical methods of decontamination (e.g autoclaves); and

— *the need to maintain the required level of active compound, including deterioration over time.*

All potential waste streams and other sources of contamination should be identified and documented. Risk assessment should be an integral part of the process to identify and develop effective decontamination regimes.

In planning and conducting decontamination activities the organization should consider:

— *ensuring that all disinfectants used contain sufficient active compound to address the working conditions under which they will be applied, and that such concentrations are maintained throughout the process, including conducting specific validation activities where necessary;*

— *providing adequate facilities and procedures for the storage of waste (including short term storage);*

— *ensuring methods are available for effective decontamination of mixed waste (e.g. infected animals that have received radioactive materials);*

— *ensuring that where appropriate, methods are available for decontamination of sensitive equipment or that which is not suitable for autoclaving (e.g. computers);*

— *implementing monitoring measures to ensure the methods have been effective (e.g. cycle recording and use of indicators in autoclaves);*

— *decontaminating protective clothing by appropriate means prior to leaving the facility;*

— *ensuring adequate methods and resources are available to deal with routine work and any spillages or other incidents during handling and transport of materials inside and outside the facility;*

— *implementing programmes to ensure the amount of contaminated waste is minimized; and*

— ensuring all personnel are trained in the use of decontamination protocols.

Records of decontamination / inactivation activities and validations should be used to demonstrate the effectiveness of the decontamination / inactivation processes.

4.4.4.5.3 Waste management

The organization shall establish and maintain an appropriate waste management policy for biological agents and toxins.

To ensure that waste is properly managed and disposed of in a safe, efficient and cost effective manner and to ensure any biological waste which may have additional hazards (e.g. radioactivity) is investigated, considered, and addressed.

Identify:

— roles and responsibilities;

— nature of the waste (e.g. liquid or solid waste);

— the appropriate decontamination processes; and

— local and environmental waste management policies.

The following elements should be considered for inclusion in a waste management policy:

— *ensure programme is in place to minimize the waste production;*

— ensure effective waste audit trails are in place and documented;

— *The organization should have a validated procedure for the inactivation of biological agents and toxins waste products* (section 4.4.4.5.2).

— *provide adequate facilities and procedures for the storage of waste (including short term storage);*

— *ensure methods are available for effective segregation and decontamination of mixed waste (e.g., infected animals that have received radioactive materials);*

— *ensure appropriate packaging material is used to contain the waste and to maintain its integrity during storage and transportation;*

— decontamination processes as required by the specification of the waste;

— effective liaison routes to local authorities for disposal of the decontaminated waste; and

— maintain appropriate levels of safety and security until the biological agents or toxins are inactivated or waste is decontaminated.

Documentation relating to the above includes:

— records of a documented waste management policy;

— records of waste audit trails;

— records of validation of waste inactivation; and

— records of waste disposal, e.g. incinerator tracking records.

4.4.4.5.4 Clothing and Personal Protective Equipment (PPE)

The organization shall ensure that PPE needs are identified and suitable equipment is specified, made available, used and maintained appropriately within the facility.

An effective PPE programme fully understood and adhered to by employers protects staff from the hazards to which they could be exposed. The organization should select PPE for laboratories based on specific risk assessment data, evaluation and analysis. In case several residual risk hazards are present, selection of the PPE should be prioritised for the most hazardous agent, and combination effects should be taken into account (e.g. solvent use reduces protection by latex gloves).

Personal protective equipment should be used in conjunction with - but never as a substitute for - reasonable and appropriate administrative and engineering controls. PPE should be used in accordance with established standards and manufacturers specifications. PPE should be made available by the employer at no cost to the employee.

Measures in place should include;

a) ensuring adequate information is used in selecting PPE (e.g. risk assessments, review and analysis of tasks, employee feedback, etc.);

b) ensuring all personnel who need *to use PPE (including scientific staff, visitors and contractors) are identified and supplied with correct fitting equipment and clothing;*

c) explicitly addressing selection and use of PPE in SOPs, training and competency assessments;

d) defining and conducting an appropriate programme to ensure that routine checks and maintenance of PPE are defined and carried out;

e) defining and addressing the need for and provision of replacement and spare PPE;

f) identifying and controlling the hazards associated with PPE itself (e.g. impaired dexterity or visibility);

g) providing adequate PPE for use during both normal and emergency working conditions;

h) ensuring procedures are in place for the cleaning and, if appropriate, the validated decontamination of used PPE including the safe storage prior to decontamination and after use.

To implement this process ensure that the following procedures are in place:

— verification of the PPE against specific agent being worked with;

— investigation of other non-biological hazards that may be present and consideration of their possible affect on personal protective equipment considered for protection against biological hazards

— assessment of protection level provided by the selected PPE;

— supply of PPE, should be available at all times;

— cleaning and maintenance of PPE;

— PPE training;

— Periodic fit testing;

— donning and doffing / removal;

— assuring that staff are following all established PPE procedures; and

— evaluation of allergic issues or medical conditions associated with PPE.

The result is an effective PPE programme working in conjunction with, but never as a substitution for elimination, substitution, engineering and administrative controls that protects employees from the hazards to which they are exposed and that the elements of this programme are fully understood and adhered to by employees.

4.4.4.6 Worker health programme

The organization shall ensure that risk to worker health, and that of other personnel whose health could be directly impacted by exposure to biological agents and toxins, is managed effectively including prevention and protection measures.

The requirements of the health surveillance programme shall be determined by a defined health hazard identification and risk assessment process involving all relevant personnel.

The organization should do all that is reasonably practicable to prevent detrimental health effects due to workplace exposures. In the framework of biorisk management this includes prevention of infection, health monitoring, and post exposure treatment. A preventive occupational health programme helps to reduce the likelihood of an employee becoming sick due to work-related exposure to chemical, physical, infectious or toxic agents. A good treatment programme helps to reduce the consequences of staff infected while working with biological agent (s).

The worker health programme should address the needs of all individuals who may be associated with the facility, including providing assurance that contractors and visitors receive the required level of protection in line with the activities they will perform, as well as safeguarding workers' families.

Typical components of a worker health programme may include:

— consultations from *relevant personnel* that may include:

a) the biorisk management advisor;

b) the occupational health professional;

c) facility personnel and employee representatives;

d) external experts, including emergency responders;

e) biorisk management committee members;

f) veterinary and animal care facility staff;

g) human resources representatives;

h) communicable disease specialist; and

i) scientific management.

— health monitoring programme based on the risk of the biological agent;

— agent inventories;

— type of techniques used and experience level;

— type of manipulations;

— characteristics of the facilities;

— pre-employment and ongoing health status of personnel;

— protection measures in place;

— processes in place;

— prior exposures or pre-existing disease states;

— necessary accommodations;

— inclusion / exclusion criteria, where applicable;

— SOPs;

— job descriptions;

— updated medical histories of staff;

— workflows; and

— available financial resources;

The process to implement this should include:

— *identification of personnel considered to have significant risk of exposure and assessment of their healthcare needs, including need for vaccination, PPE Provision and emergency measures such as isolation / testing in the event of exposure;*

— *consideration of the health and immune status of individual;*

— establishment of *appropriate work conditions with periodic checks of* work areas*;*

— addressing *other conditions that could impact personnel associated with the facility, including their ability to use appropriate PPE safely, medical conditions or factors affecting their general well-being (e.g. epilepsy, heart attack, impaired vision, physical mobility / dexterity, stress, depression, pregnancy, immune status, etc.)*;

— *information covered by worker health programme should be treated in confidence;*

— *all individuals should have access to healthcare consultations with either a corporate or institutional occupational health facility or an independent health care provider, and be informed as to the nature of any treatments / vaccinations they may receive and the inherent risks and benefits of these treatments / vaccinations;*

— medical response plans for all biological agents and toxins the facility handles;

— identification of available vaccines and their side effects;

— vaccination strategy;

— decision on the appropriate use of serum banks;

— identification of prophylaxis and post-infection treatments available and where they should be stored; and

— communication methods with local medical service providers;

The outcome consists of:

— a comprehensive occupational medical programme relying on prevention, as well as contingency plans for emergency situations;

— provision of emergency contingency plans that also cover contractors and visitors; and

— increased awareness or provision of information to staff on the potential risks associated with their work or the agent that they are handling and the likely consequences (e.g. sign symptom) of exposure to such agents.

4.4.4.6.1 Vaccination of personnel

Based on risk, the need for vaccination shall be identified and shall cover groups identified as being potentially exposed to biological agents or toxins.

The organization shall ensure that a vaccination policy be defined and implemented, and that access to laboratories or work is controlled for individuals until they comply with the policy.

The organization should do all that is reasonably practicable to prevent infection of its staff. A preventative occupational health programme helps inform an employee of the infection risks associated with working with designated biological agents and toxins and the benefits of pre-exposure vaccination.

The set-up of a vaccination programme may include:

— a list of the biological agents that the facility works with, including those potentially present in samples routinely analysed in the facility, which are different from the usual targets of the analyses;

— an inventory of source and availability of vaccines;

— vaccine efficacy and safety data such as vaccine approval and testing information;

— a list of personnel to be vaccinated based upon risk assessment of their work activities and organisms they handle;

— policy for pre-employment vaccination;

— policy for pre- or post-exposure vaccination;

— policy for individuals with a low titer / response to the vaccine and for individuals unable to receive the vaccine; and

— policy for the use of vaccines in early stages of clinical development for selected infectious agents (e.g. where the medical consequences are severe if exposure goes undetected).

Measures should be implemented to identify non-responders to vaccination when needed (depending on the response rate of the vaccine) and a policy should be in place to address these individuals.

— *Individuals considered unfit for work in the facility on health grounds should be identified and prevented from accessing areas where there are risks of exposure.*

— *Areas requiring vaccinations* for *entry should be* identified and *posted*.

— Visitors, contractors and other non-core personnel should provide evidence of vaccination or evidence of established immunity in accordance with the above requirement.

— Based on risk, reasonable measures should be taken to ensure that the vaccinations have been given and current certificates are valid. This may include examination of original certificates and crosschecking with medical practices responsible for administering the vaccine.

— The organization should ensure that the required or recommended vaccines are made available to the concerned personnel.

— *Vaccination should be seen as a risk-mitigation strategy and* an administrative control that reduces the risk of infection but does not *infer that* other *controls* identified in the risk assessment *be relaxed, i.e., good microbiological technique,* engineering, and *PPE.*

The result is a comprehensive vaccination programme that ensures the health of employees working with biological agents.

4.4.4.7 Behavioural factors and control of workers

The organization shall establish and maintain a programme to address risk associated with human behaviour, including the management of how workers interact with the facility and its equipment.

The organization should ensure that behavioural factors and the need for individual support and communication are managed responsibly and sensitively*. Many laboratory incidents are caused by inappropriate behaviour or human frailties, and a* preventative *approach to managing risks associated with individuals should be pursued, including the specific inclusion of such issues in risk assessments. The use of* a multidiscipline approach *in assessing this area should be considered* to promote safe behaviours.

Typical examples include:

— SOPs;

— employment health and safety (EHS) programmes; and

— biorisk management policy.

Measures should be set in place to address:

— training of managers to recognize human factors considerations and observing their signs within their work force;

- *human reliability and behavioural safety practices, including adherence to procedures;*
- *communication, consultation, and feedback;*
- *conflict management and resolution;*
- *empowerment, including authority to stop work if potentially unsafe or unsecure conditions are identified;*
- *avoidance of a "blame culture," including* freedom *to report accidents, incidents or unsafe conditions* without fear of reprisals;
- *ergonomics, including equipment and work practice designed to take account of individual needs; and*
- *respect for individual privacy and dignity.*

The organization should encourage proactive management to shape behavioural control measures through the promotion of open communication practices. Corrective action may be needed in some instances; any corrective action should be documented and follow a strict procedure.

4.4.4.7.1 Personnel reliability

The organization shall ensure that a personnel reliability policy is defined and implemented and that access to facilities or work is controlled for individuals according to the policy.

The organization should develop and implement a system that includes different levels of personnel screening based on job responsibilities and should be periodically reviewed. The personnel reliability system should be based on applicable local and national legal and regulatory frameworks, human resource recruitment practices, employment requirements and occupational health and medical requirements.

The nature, extent and type of *measures required* to assess *personnel reliability should be determined* by *the risk assessment process* and management policy. Different positions at the facility may involve different levels of risk, and thus may require different levels of personnel reliability screening. For some positions, checking *employment references* and verifying competence or expertise may be all that is necessary. For *other* positions, *more in-depth* personal background *screening may be deemed necessary*.

Where lawful and appropriate as determined by the risk assessment, screening may include checks on *identity and immigration status, membership of organizations hostile to biological research, criminal records,* drug screening, *and financial probity.*

Periodic reviews should be undertaken to assess changes in job responsibility and / or the ability to carry out those responsibilities; appropriate actions should be taken in response to those reviews.

Ultimately, management is responsible for ensuring that those they supervise are fit for duty and adequately qualified and trustworthy to execute their job responsibilities. Management should define and document the various positions at the facility based on the risk assessment process and management policy. The facility should have a graded personnel reliability system where the depth of the review reflects the level of risk associated with the position held. The specific requirements of the personnel reliability system should be consistent, transparent, and documented. The results of personnel reliability screening measures should be treated as sensitive information, confidential, and protected accordingly.

4.4.4.7.2 Contractors, visitors and suppliers

The organization shall ensure that suppliers, contractors, visitors and sub-contractors adhere to the requirements of established management systems and do not compromise biorisk management of the facility.

The organization's biorisk management policies should include processes and procedures designed to address contractors, visitors, and suppliers who enter and / or work in the facility to ensure their safety and also the security of the facility's materials and operations.

Biorisk management policies that address the implications of competent suppliers, contractors, and visitors should be based on the facility's security and safety requirements, its purchasing, maintenance and service requirements, clear selection criteria, visitor policies, and risk and threat assessments.

The organization's biorisk management policies should describe procedures that govern how contractors, visitors, and suppliers can access specific areas of the facility or specific equipment (requiring permits). These procedures should be based on facility risk assessments, and, if necessary, designate areas that contractors, visitors, and suppliers can access only if escorted by an approved facility employee. Access to certain, higher risk areas of the facility may also be governed by the time of day, the day of the week, the type of work being performed, the clearance level designated by management, or other criteria.

The organization's management should identify those employees who are approved to escort contractors, visitors, or suppliers to certain, higher risk areas of the facility. Those employees who are approved to escort contractors, visitors, or suppliers should be trained on the safety and security implications of escorting these individuals into the facility. In addition, the contractors, visitors and suppliers might also require training to be escorted into high-risk areas of the facility. The organization may choose to allow some but not all contractors, visitors, or suppliers' access, either unescorted or escorted, to certain, higher-risk areas of the facility.

These procedures, as well as site-specific hazard awareness and hazard recognition requirements, should be clearly communicated to facility employees and the organization's contractors, visitors, and suppliers through training and other information in advance of their access to the facility. This also should be clearly documented in the organization's biorisk management policies. Execution of these policies should help ensure that suppliers, contractors, and visitors conform with the biorisk management system.

4.4.4.7.3 Exclusion

The organization shall ensure that measures are set in place for the removal and exclusion of personnel (both temporary and, if appropriate, permanent) from the facility where deemed necessary through risk assessment.

The organization should have an adequate security system in the facility to exclude any individuals who do not have legitimate access and a procedure for removing the legitimate access of individuals that present a security risk, including own staff.

It should be clearly communicated that there are consequences to any individual (e.g. visitors, contractors, students, employees) if they violate certain criteria, in accordance with local laws regulations and organization's policies.

The organization should define the process for exclusion, including:

— exclusion criteria and persons authorized to action exclusion;

— *removal of access to the facility (e.g. removal of passes, changes of keys, access codes and other security devices, etc.);*

— *removal of access to information relating to the facility including documentation, computerized records and data; and*

— *immediate physical removal of personnel if deemed necessary.*

SOPs that clearly define exclusion processes for unauthorized individuals should be communicated to all staff and those visiting the facility.

4.4.4.8 Infrastructure and operational management

The organization shall ensure that facilities, equipment and processes are designed and run in a safe and secure way with respect to biorisk management.

Facilities, equipment and processes are designed and maintained for safe and secure operation to address risk, including biorisks.

Design and redesign of facilities and processes and the selection of equipment should consider the following:

— a risk analysis of the proposed changes;

— validation that design, equipment and processes are consistent with biorisk assessment;

— facilities and equipment are designed to operate and be maintained in a sustainable and efficient manner;

— consultation of future facility stakeholders or uses and functions (needs); and

— acceptance criteria for design, construction and operation.

Documentation for the facilities, equipment and processes should include:

— the use and function of the facility;

— relevant national and international standards, regulations, and guidelines;

— original and redesign drawings and specifications;

— operation / maintenance manuals and procedures;

— commissioning documentation; and

— operation, maintenance, calibration and validation history.

To evaluate the safety and security of facilities, equipment and processes, the following documentation should be available:

— validation reports;

— biological incident reports related to design, equipment or processes;

— operational and maintenance costs;

— number and nature of facility, scientific and safety equipment failures;

— number and nature of security failures; and

— failure of continuity of operations.

4.4.4.8.1 Planning, design and verification

The organization shall ensure that a formal planning, design and redesign process is adopted for the facility, based upon an assessment of risk associated with the materials to be used and activities undertaken.

The design process shall identify and incorporate all relevant legislative requirements, together with information from recognized standards, guidelines, industry good practices and facility-specific risk assessments.

The design process shall identify and consult all relevant parties associated with the facility and its operation.

All design features, construction techniques, materials and equipment selected shall be documented in line with the need to provide sufficiently specific and detailed instruction and information on the design specification.

The organization shall ensure that a new construction and physical facility modifications are carried out according to an approved plan.

— to ensure that facilities, equipment, processes are planned and designed with respect to the use, function and biorisk management of the facility; and

— a facility that meets the acceptance criteria in accordance to the approved plan.

A formal design process means a structured and documented approach whereby the needs of the facility are determined through risk assessment. Engineering and operational solutions should *be incorporated that are consistent with the risk posed by the properties of materials that will be stored and handled in the facility and the nature of the work to be carried out.*

Typical aspects include:

— the use and function of the facility;

— ensuring space is properly designed so that the facility, scientific and safety equipment can be properly maintained and / or removed;

— planning and documentation verification process for the new facility;

— staff consultation on the design, construction, inspection and verification of the new facility;

— budget planning documentation of the process to ensure there are adequate resources for construction;

— planning and documentation for the facility specific risk assessment;

— relevant legal requirements and codes of practice; and

— planning and documentation for the design, redesign, construction, inspection and verification processes for the new facility.

The design process should include the identification and review of relevant legislation and codes of practice (including building codes as well as those relating to laboratory biosafety / laboratory biosecurity) and risk assessments. The requirements identified from these sources should be incorporated in the design plans. The design should be fully documented, including a description of the tests and the standards of acceptance to assure performance. The process should be documented and transparent to provide an assurance that it has been comprehensive and thorough.

The design process should include the identification of and consultation with individuals involved in planning, construction and operation of the facility and its future use.

The project owner should formalize a project committee for defining the use and needs of the facility, and providing input to design and commissioning specifications. The project committee membership *should consider representatives from:*

— management;

— *scientific* leaders */ personnel*;

— laboratory technical staff / *other end users*;

— *maintenance engineers /* technical staff;

— HSE / biosafety staff (*biorisk management advisor, biorisk management committee, biosecurity and / or security personnel)*;

— *designers (architects and engineers);*

— *commissioning agents;* and

— financial staff.

Additionally, *the following roles / individuals should be considered in terms of information* requirements *and need for consultation:*

— *constructors;*

— *materials and equipment suppliers;*

— pest management consultants;

— *certifiers;*

— *regulators*, including local authorities*;*

— medical *and first responders*;

— community representatives; and

— *other relevant parties identified in risk assessments.*

If justified on the basis of the nature of the work, a peer review process involving independent, competent third parties should be conducted to ensure that the design specification:

1. *is in line with accepted* building and engineering *good practice*;

2. *incorporates features capable of providing assurance for the control, storage and security of biological agents and toxins; and*

3. *ensures relevant legislative requirements, standards, and risk assessment findings have been incorporated into the design.*

Documentation that should be available as a result of the above includes drawings and specifications that reflect the planning, design and verification requirements and change requests.

4.4.4.8.2 Commissioning and decommissioning

The organization shall ensure that there is a formal process for initial commissioning of new facilities and the final decommissioning of existing ones.

Commissioning will ensure that the facility is constructed and performs as intended.

During the construction process the organization should ensure that the components, equipment and system of the facility operate as designed and specified. Commissioning ensures a building's operational integrity and performance as designed. When an organization has decided that a facility or equipment is no longer sustainable, a decommissioning plan should be developed to carry out the process safely and cost effectively.

The commissioning process should start at the design phase at the first stage of science programme definition to assure that the expectations for the building are achievable. The commissioning plan should develop in detail in parallel with the physical concept to ensure that the expectations for the building are measurable. The commissioning plan should clearly identify, with examples, all steps from beginning to end including conditions of acceptance of each step as a prerequisite of proceeding to the next. The commissioning plan should identify all steps required before operation is commenced initially or resumed after temporary shutdown.

The commissioning process should provide the benchmark for acceptable facility operation and the description of the programme to be put in place to maintain that level of performance.

Written procedures on the following should be considered:

— integrated system testing;

— equipment testing;

— components testing; and

— verification of the structural integrity of the facilities according to acceptable criteria or local building regulations.

The decommissioning process should identify the decontamination procedures and security-related measures that have to be in place for temporary or final shut down of the facility. The decommissioning programme not only should describe the procedures to be undertaken but also the standards of acceptance when those procedures are performed. This may be documented through clearance certificates and permits to work which identify when and under *what conditions the decommissioned facility can be re-entered.*

When possible the organization may consider having an independent third party perform the commissioning and decommissioning of the facilities.

Documentation that should be available as a result of the above is a commissioning report that details the operational, adjustment and testing characteristics of the facility, systems and equipment as designed and specified. Where applicable the decommissioning plan and verification that the decommissioning process has been completed safely also should be documented.

4.4.4.8.3 Maintenance, control, calibration, certification and validation

The organization shall establish and maintain documented procedures to ensure equipment and elements of the physical plant that may impact on biorisk be identified, purchased, maintained, calibrated, certified or validated in a manner consistent with the intent and requirements of the biorisk management programme.

To ensure that there are documented procedures for equipment and all aspects of the physical structure consistent with the requirements of the biorisk management programme including:

— maintenance;

— control;

— calibration;

— certification; and

— validation.

1. Maintenance:

The maintenance programme should apply to all aspects of the physical structure and grounds *(including finishes and seals where appropriate) and equipment therein. All materials used should be specified to ensure they can perform in line with predetermined criteria. An appropriate maintenance plan will be addressed as part of that specification process.*

Maintenance (preventative or predictive) should be performed in accordance with the programme and the manufacturer's recommendations. Reactive maintenance is undesirable because it increases risk and should be avoided.

In planning and conducting maintenance activities the organization should consider:

a) adequately maintaining the physical integrity of the facility and its fixtures and fittings;

b) ensuring maintenance activities are performed by competent individuals, and that risks associated with the work have been subjected to risk assessment;

c) identifying and recording maintenance requirements at the time of construction of facilities, or purchase / acquisition of equipment;

d) creating and maintaining a maintenance register for all applicable equipment;

e) identifying and conducting planned maintenance activities at an appropriate frequency;

f) ensuring adequate provision for unplanned (breakdown) maintenance to ensure integrity of the facility is maintained at all times;

g) determining and monitoring predictive maintenance requirements and associated indicators and monitors;

h) ensuring essential spare parts are available in line with a frequency appropriate to the risk of failure and need for replacement; and

i) a pest control programme.

2. Controls:

In planning and conducting equipment controls, the organization should consider:

a) identifying equipment in line with identified work needs which can be demonstrated as fit for purpose;

b) controlling purchase / acquisition / transfer of equipment to ensure all necessary risk assessments are completed and approval is authorized by competent personnel;

c) controlling entry and exit of equipment to and from the facility, including decontamination requirements (e.g. air locks and decontamination);

d) documenting equipment, material and waste;

e) adopting an audit trail system for equipment, material and waste; and

f) establishing and maintaining an inventory of all facility and scientific equipment, including critical spare parts and consumables.

3. Calibration:

In planning and conducting calibration activities, the organization should consider:

a) identifying and recording calibration requirements at time of purchase / acquisition;

b) identifying the standards / tests that will be used to ensure the equipment is correctly calibrated;

c) creating a documented and up-to-date calibration register for all applicable equipment;

d) ensuring calibration for identified equipment is scheduled and conducted in line with manufacturers' recommendations and / or other specified intervals as identified by risk assessment;

e) completing all calibration documents and keeping them on file for future records; and

f) addressing calibration requirements for quality assurance management systems (such as ISO 9001, ISO 15189 and ISO 17025).

4. Certification:

In planning and conducting certification activities the organization should consider:

a) identifying and recording certification requirements at time of purchase / acquisition of equipment, including relevant and current standards against which to certify;

b) ensuring competent and independent certifiers (large institutions may have in-house certifiers*) are used for the certification process;*

c) ensuring certification is scheduled and conducted in line with manufacturers' requirements and / or other specified intervals as identified by risk assessment;

d) performing certification of identified equipment;

e) ensuring re-certification is performed following major repairs and relocation of equipment (if required); and

f) ensuring re-certification is performed at the required intervals.

5. Validation:

In planning and conducting validation activities, the organization should consider:

a) identifying and recording validation requirements at time of purchase / acquisition;

b) identifying the standards / tests that will be used to ensure the equipment is correctly validated;

c) creating a documented and up-to-date validation register for all applicable equipment;

d) ensuring validation is scheduled and conducted in the line with manufacturers' requirements and / or other specified intervals as identified by risk assessment;

e) ensuring competent and independent validation companies (large institutions may have in-house validation groups) *are used for the validation process; and*

f) performing the required tests for the validation.

Note that validation tests are required for certification.

6. Emergency response plans (section 4.4.5) should be in place in the event of:

a) failure of building management system or building automation system;

b) equipment failure;

c) multiple equipment failure;

d) utility failure; and

e) anything affecting ongoing containment such as natural disasters, etc.

For physical security systems, the analogous concept is performance testing; evaluating the entire physical security system (equipment, policies, procedures, and people) to ensure the system works as designed.

4.4.4.8.4 Physical security

The organization shall ensure that the controls for the physical security of cultures, specimens, samples and potentially contaminated materials or waste determined as part of the risk assessment process are implemented and maintained.

Measures should be set in place to minimize the potential for release or removal of biological agents from the facility due to a breach in security. This should involve proactive measures to identify vulnerabilities and implementation of effective control and monitoring mechanisms.

The organization should implement a comprehensive physical security system that includes graded protection of all hazardous materials and reflects the results of risk and threat assessments.

The physical security system should reduce the risk that biological agents might be maliciously removed from the facility. The physical security system also should support the facility's biosafety system by limiting access to areas where there are biological agents and toxins to those employees who are qualified, trained, and approved to conduct work with those materials. The physical security system should be graded or designed so that risk security scenarios, based on the risk assessment process, are protected at a higher security level than the lower risk security scenarios.

The physical security system should include provision for the regular testing and maintenance of all security measures to ensure that they are performing as expected. The physical security system should regularly review applicable risk and threat assessments to ensure that the mitigation measures appropriately reduce the risk of loss or theft of valuable biological materials. These regular evaluations of the physical security system should be documented and protected.

The physical security system should be based on, but not limited to, the following documents, policies, and requirements:

— risk and threat assessments;

— facility engineering and architectural plans;

— biosecurity plan;

— biological agents and toxins inventory;

— biological agents and toxins containment procedures and policy;

— personnel, visitor and contractor access policies;

— regulatory requirements;

— personnel clearances;

— publications;

— patient data; and

— control systems.

The organization should identify the physical location where hazardous materials, sensitive information, or critical systems will be used and stored. The organization's physical security system should secure materials in those physical locations, ensuring that only authorized personnel have access to those locations and preventing or detecting access to those locations by unauthorized personnel. The physical security system should also establish a method for immediate notification of emergency responders in the event of a security breach.

In planning and conducting security risk assessments, the organization should consider:

— *theft or diversion of biological agents and toxins or related equipment, documents or data;*

— *sabotage including vandalism and tampering;*

— *break-in and intrusion;*

— *labor issues and disputes;*

— *weather-related emergencies (i.e., earthquake, tsunami, flood, tornado, and hurricane);*

— *workplace violence;*

— *utilities failure;*

— *picketing, occupation and barricade;*

— *screening and isolation of suspect packages;*

— *acts of terrorism; and*

— *civil unrest or war.*

Care should be taken to coordinate biosecurity measures with those of biosafety to manage and minimize conflicting priorities.

4.4.4.8.5 Information security

The organization shall have a policy and procedure in place to identify sensitive information; a review and approval process shall be used to control access to such information.

The information generated by a laboratory can be as valuable and / or dangerous as the biological agents and toxins stored at the facility. The organization should implement appropriate *measures to prevent unauthorized* access to, or *release of, such information*. The organization should implement a comprehensive information security system that includes graded protection of information that reflects the results of risk and threat assessments.

The information security system should be based on, but not limited to, the following documents, policies and requirements:

— risk and threat assessments;

— information technology plans;

— biosecurity plan;

— personnel, visitor, and contractor access policies;

— regulatory requirements; and

— personnel clearances.

The information security system should:

— protect more sensitive information more securely than less sensitive information;

— determine who will have access to the different security levels of information among employees and the general public and how that access will be managed; and

— include guidelines for marking, storing, transmitting, transporting, and destroying sensitive information.

The organization should clearly define the roles and responsibilities of those employees who are responsible for designing, implementing, and maintaining the information security system.

The information security system should define the organization's process for identifying sensitive information. Some information owned and controlled by the organization may be more sensitive than other information. The most sensitive information might include details about the facility's security system and its personnel records, for example. The process for identifying the sensitivity of the organization's information should be documented and communicated to the organization's employees through training and other means.

The *procedures for addressing information security should consider*:

a) secure storage of all sensitive written records and data, including electronic records and electronic signatures;

b) computer security including robust internet firewalls and encryption protocols;

c) strict policies regarding personal computers *(PCs), laptop computers,* personal phones, tablet computers*, storage media, cameras, etc. entering or leaving the facility;*

d) thorough destruction of paper files to be discarded and complete erasure of unwanted electronic files; and

e) security measures and procedures.

The organization's information security system should define what risk mitigation measures are used to protect sensitive information. This system should ensure that these measures are regularly tested and maintained to ensure they are performing as expected. The information security system should regularly review applicable risk and threat assessments to ensure that the mitigation measures appropriately reduce the risk of loss or theft of sensitive information. These regular evaluations of the information security system should be documented and protected.

4.4.4.8.6 Control of supplies

The organization shall ensure that purchases (including services) conform to specified requirements. Controls shall be applied depending on potential impact on the biorisk involved.

The organization shall ensure suppliers are evaluated and selected based on their ability to provide products / services that meet the requirements of this standard. Criteria for selection, evaluation and re-evaluation shall be established. Records of the results of evaluations and any necessary actions arising from the evaluation shall be maintained.

While not all suppliers will provide products / services that may impact on biorisk, there are many that may. The organization should develop a process to evaluate suppliers and services and all purchases to ensure they meet the requirements of safety and security, including the biorisk programme of the facility. *Suppliers that should be considered include, but are not limited to, those that provide:*

a) cleaning services;

b) laboratory equipment, apparatus and consumables;

c) waste management or disposal services;

d) I T (information technology) *support services;*

e) equipment and facility maintenance services; and

f) security services.

The suppliers and services evaluation process may include:

— the requisite competencies of suppliers, contractors, and subcontractors accessing the facility to perform work needs to be determined, and parties accessing the facility must demonstrate their possession of these competencies;

— development of specific biosafety and biosecurity criteria in the specifications of the supplies and services being procured;

— prequalifying of suppliers and service providers for commonly procured supplies and services;

— requiring the providers of supplies and services to certify that their products and services meet the requirements of the biorisk management plan; and

— ensuring deviations from the requirements are identified, and their impacts on the biorisk management plan are evaluated before services or supplies are utilized.

The organization should develop a review and approval process for all purchases to assure that all purchases meet the facility's safety and security including biorisk requirements are met based on documented procedures for procurement of supplies and services.

These reviews should take into consideration legal and permit requirements (e.g. shipping documents, permits, acceptance testing, quality control) and the risks associated with the materials and services intended to be purchased.

4.4.4.9 Transport of biological agents and toxins

The organization shall ensure that procedures for the safe and secure transport of cultures, specimens, samples and contaminated and potentially contaminated materials are established and maintained in accordance with legal requirements for the transport of dangerous goods.

To ensure the safe and secure transport of biological agents and toxins.

In planning and conducting transport activities the organization should consider:

a) ensuring transport requirements are identified and implemented, including legal requirements and national and international guidelines;

b) ensuring adequate packaging systems, materials, labels, PPE and documentation are available and used as part of the transportation process;

c) selecting a reliable, trustworthy carrier that is qualified to handle the package safely and securely;

d) determining *whether a request for biological agents and toxins or material that may contain viable biological agents is being made by an approved facility for a legitimate reason, and equivalent controls are applied to importation of material to the facility;*

e) the need is identified for formal transfer documents signed by the responsible management representative authorizing movement of materials;

f) document control that allows traceability of material movements;

g) identifying and implementing adequate and proportionate emergency response and contingency plans associated with transportation, including adequate precautions for handling suspicious packages, quarantine areas and appropriate explosive stand-offs; and

h) nominating and training a transport safety advisor who should be aware of the specific carrier requirements for a biological agent shipment.

Documents that should be available as a result of the above include:

— written acknowledgement by the receiving organization that the material was delivered and in a safe and secure condition (the document audit trail);

— written acknowledgement from carrier that they have an appropriate security plan for the materials being transported; and

— documentation of staff training in transport of biological agents (Transport of Dangerous Goods training).

4.4.4.10 Personal security

The organization shall have a policy in place to provide personal security support services to staff members that include, where appropriate, personal security awareness training.

Personal security is concerned with staff security during off-duty hours while away from the facility. During these times, staff members are vulnerable because of their function or position.

Personnel may be vulnerable to threats, physical attacks, etc. to themselves or their families or property by virtue of their function or position at the facility. The organization should take steps to identify and assess these vulnerabilities and can implement a process to address these issues, such as general personal security awareness training and counterintelligence training when considered appropriate. As the external and political environment may change over time, regular reviews of these threats, vulnerabilities, and mitigation measures should be conducted.

4.4.5 Emergency response and contingency plans

The organization shall establish and maintain plans and procedures to identify the potential for incidents and emergency situations involving biological agents, toxins and materials, to prevent their occurrence, to respond to emergency situations and to limit the likely illness or other damage that may be associated with them.

Emergency planning shall cover all aspects of biorisk and include general safety, security and medical issues.

To ensure the safety of staff members, visitors, vendors and the surrounding community, the organization should actively assess potential incident and emergency response needs, develop procedures and processes to cope with them, and continually aim to improve the effectiveness of responses.

Emergency response plans may include but are not limited to:

— risk assessment data necessary to begin the emergency response planning process;

— identifying and assigning roles to and responsibilities of staff members in the event of an emergency;

— identifying roles and responsibilities of people involved in emergency management;

— identifying and listing (inventory) of readily accessible emergency equipment, including location and maintenance status;

— assessing the availability of local emergency responders;

— a list of regulatory bodies to report to, depending on the level of emergency;

— information from consultation and planning sessions with local emergency responders;

— experience from previous accidents or incidents at the facility or from similar facilities;

— accident and incident investigation reports (lessons learned);

— review of emergency drills and exercises;

— informational signage related to emergency response such as evacuation routes, exit signage, location of emergency response equipment, etc.;

— development of emergency plan(s) using risk assessments, scenarios and consultation with local responders;

— identifying necessary emergency equipment provided to responders and periodically testing its suitability;

— procedures for reviewing and capturing lessons learned following each incident or emergency response event in order to improve future performance;

— procedures for coordinating response plan processes and resources across organizational, municipal, governmental levels, etc.; and

— providing training to staff in indigenous language.

Emergency plans will include evacuation procedures and maps, communication plans (including phone numbers, frequencies and other contact information), operational continuity plan, plans for hazardous materials in the event of an emergency, creation of emergency equipment inventory (threat detection, fire fighting, safety, security, communication and power back up) and storage of emergency equipment in a safe and accessible location.

4.4.5.1 Emergency scenarios

The organization shall ensure that all credible and foreseeable emergency scenarios that may impact the organization's biorisks have been identified.

The organization should identify potential accident and emergency scenarios in order to develop and validate planned responses.

In order that emergency planning can take place, it is necessary to consider all credible emergency scenarios. It is unlikely that all potential scenarios will be credible; however, all reasonable threats should be considered and recorded and, where appropriate, the rationale as to why issues were dismissed.

A list of possible emergency *scenarios* that could affect the facility might *include:*

— *infected / potentially infected worker or other contact (e.g. family member, emergency responder or community member;*

— *accident or illness to worker and need for evacuation;*

— *fire;*

— *flood;*

— *breach of security;*

— *explosion;*

— *potential loss of biological agents or toxins through theft or any other reason;*

— chemical spill;

— *unexpected virulence (unknown biological agents or biological agents expected to be avirulent);*

— theft or spill of radioactive materials;

— *physical facility and equipment failure, including control system failure;*

— *failure of disinfection regime;*

— *utility failure including electricity, gas, steam and water supplies;*

— *major spillage / aerosol release;*

— *environmental release;*

— *natural disaster (e.g. earthquake, extreme weather conditions, disease pandemics etc.);*

— *act of terrorism or deliberate vandalism;*

— *intense media attention; and*

— loss of communication systems.

Review all possible scenarios, document conclusions, and move forward for those deemed credible to your facility.

4.4.5.2 Emergency plans

The organization shall ensure that biorisks are taken into account when preparing and implementing emergency plans.

The organization shall ensure a system is established to effectively manage medical and/or environmental emergencies, including, but not limited to, the identification of potentially infected workers and provision of immediate medical care to exposed, ill or injured workers.

The organization shall also ensure that control measures in place can be demonstrated as being reasonable and proportionate to the scale and nature of the emergency.

Emergency plans shall be effectively communicated to all employees and relevant third parties, and tested, with the intention that everyone is aware of their obligations.

The organization should develop emergency response procedures for all credible scenarios and continually aim to improve the effectiveness of responses.

Components of an emergency plan may include:

- Development of emergency plans scenarios using:
  - identification of the location of hazardous materials and the emergency action required;
  - *risk assessments data;*
  - lessons learned from previous emergency response activities to improve effectiveness of response procedures;
  - information from consultation and planning sessions with local emergency responders;
  - identifying measures to control environmental impacts;
  - making relevant information available during the emergency (building layouts, location and nature of hazardous materials data where examples include material safety data sheets, laboratory containment level, contacts information); and
  - information from emergency and practice evacuation drills.
- Assignment of roles and responsibilities and a chain of command and consider:
  - identification of people in charge during the emergency (chain of command in accordance with the level of the emergency). It also should include designation of authority of people with specific roles during the emergency (wardens, first aid staff, spill teams, maintenance, interaction with first responders, etc.);
  - involvement of relevant management levels depending on the type of emergency;
  - *the need to respond during out-of-hours emergencies as well as those that occur during normal working hours;*
  - *provision for periods of reduced staff availability (e.g. during weekends and holiday periods);*
  - *identification of those responsible for devising, implementing and testing the control measures specified*; and

- *identification, roles and availability of emergency responders:*
  - *consulting external agencies which might be involved in the response and establish their role in responding to a given situation. These may include:*
    - *police and security services;*
    - *fire services;*
    - *ambulance and local hospitals / healthcare providers;*
    - *transport providers / couriers;*
    - *local and national government officials; and*
    - *environmental authorities;*
  - *documenting contact information and making it available to personnel responsible for coordinating the emergency response activity;*
  - *informing and educating external services in their roles and any risk exposures they may face and ensure their actions will not unnecessarily increase the risk associated with the emergency (e.g. uncontrolled use of fire water);* and
  - *reviewing options to sign a memoranda of understanding or agreements with key responders;*
- *evacuation plans to include:*
  - *the need for emergency access / exit, including the ability to override access controls as appropriate and emergency exit routes to avoid evacuating people through areas of higher biosafety or biosecurity;* and
  - *provision for safe removal, transport, transfer, treatment and accommodation of contaminated persons, objects,* etc.*;*
- worker health and first aid:
  - *procedures to address worker health needs in the event of an accident or emergency situation*. *This provision should extend to first responders and their families, members of the broader community and to environmental conditions that may have been affected by the incident. This should include the identification of emergency scenarios, including infected worker / family member, together with the necessary support measures (e.g. liaison with emergency services / local authorities), provision of equipment and other resources required to manage the emergency (e.g. prophylaxis, post-exposure treatment, disinfectants, isolation requirements, vaccines, etc.). The necessary plans and other materials for managing medical emergencies should be prepared, tested and maintained;*
  - *adequacy of first aid provision in relation to credible accident scenarios identified during risk assessment. The procedures should address the need for adequate provision of trained personnel and their availability, as well as equipment and other materials that may be required in the provision of treatment;* and
  - *identification of additional available competent medical support (e.g. hospitals, isolation units, etc.);*
- communication:
  - identifying personnel knowledgeable in risk communication responsible for communicating on behalf of the facility with

- the community;
- the general public;
- the authorities; and
- the employees;

- developing communication plans and procedures for communicating specific actions to be taken by personnel at the site of the emergency, including contractors and visitors; and
- informing and educating external services in their roles and any risk exposures they may face to ensure their actions will not unnecessarily increase the risk associated with the emergency (e.g. uncontrolled use of fire water, receipt by hospital emergency of patients possibly infected with biological agents).

- emergency equipment:
  - determining the needs for/purchase of emergency equipment such as alarm systems, emergency lighting and power, means of escape, safe refuges, critical isolation valves, firefighting and first aid equipment, safety, security and backup power equipment, communication facilities; and
  - testing and documentation of emergency equipment;

4.4.5.3 Emergency exercises and simulations

The organization shall ensure that structured and realistic emergency exercises and simulations, including security drills are conducted at regular intervals, based on risk, to test the plans, prepare personnel, and learn from any good practices or deficiencies identified.

The organization should actively test its emergency plans with *exercises* involving all pertinent employees and staff *in order to provide an assurance that plans are effective and to learn from any lessons that arise*.

- Practice drills should test the effectiveness of the most critical parts of the emergency plan and the completeness of the emergency planning process. Inclusion of external organizations or agencies (e.g. local fire-fighters, police department, and county or state emergency management teams) during practice drills should be considered.
- The starting point should be the emergency plans and considerations developed under section 4.4.5.2.

Elements of emergency exercises and simulations may include:

- *planning exercises,* (e.g. desktop exercises, mock exercises, practice drills*), that are realistic representations of the events they are designed to simulate* and verify that the actions planned are effective in the event of a real emergency*;*
- *conducting exercises under controlled conditions so they are not allowed to become a source of risk in their own right;*
- evaluating *results from exercises* and drills, including security drills after each exercise and having a process *of lessons learned* in place to identify and implement modifications to the plan to ensure effectiveness and completeness;

— *providing feedback to appropriate personnel on performance;*

— *recording any actions that have arisen and allocate to named individuals;*

— *ensuring measures set in place are closed out effectively;*

— determining the frequency and type of emergency exercises and simulations, including security drills based on the likelihood of the event; and

— conducting personnel training programmes on emergency equipment use;

4.4.5.4 Contingency plans

The organization shall ensure that in the event of an emergency, adequate contingency measures shall be in place to ensure the safety and security of continued operations.

In the event of an emergency or unforeseen event there may be disruption to normal operating conditions. This could range from the need to safely shut down work in the event of a power failure, to obtaining alternative storage conditions in the event of a breakdown. Such eventualities should be considered proactively and contingency plans set in place. Activities should address plant and utility failure*, the need for adequate redundancy, replacement and other measures, which could involve the availability of alternative facilities or personnel, the introduction of backup systems (e.g. power supplies) alternative means of decontaminating materials in the event of failure of critical systems or equipment (e.g. kill tanks or autoclaves), or the complete safe shut down of operations in extreme situations.*

Contingency plans may include:

— identification of possible emergencies considered under section 4.4.5.2;

— availability of vital records and equipment and ensuring their protection;

— risk assessment data;

— lessons learned from past events;

— identifying individuals who should be notified if the contingency plan is activated, the best method for contacting them and their contact information;

— storage of critical material in two secure places;

— a list of equipment and systems that would be affected by an emergency or unforeseen events that may cause a partial or full disruption of normal working conditions;

— identification of critical areas and systems for priority response;

— identification of the possible reasons for a partial or full disruption to normal operating conditions. Prioritise these from most likely to least likely to help determine the extent and length of the disruption (i.e. power failure maybe in just one area [circuits, electrical boards], in one building, the whole area or even the entire region);

— procedures for identifying affected areas including physical locations as well as functions. These may include identification of the warning indicators (for a power failure indicators may include lights and electrical equipment not working);

— establishing a recovery time objective (minutes, hours, days, etc.) to determine when the plan should be activated to prevent major interruptions;

— checking and monitoring the status of backup resources in priority order (generator, UPS devices, access to document storage etc.) and documenting this information during each monitoring event;

— recovery of backup resources if necessary in priority order, listing the backup resources available; and

— review of potential to start work in a different location;

The result should be to produce a contingency plan that ensures normal operations are resumed as soon as possible and that any losses are minimized.

4.5 Checking and corrective action

4.5.1 Performance measurement and analysis of data

The organization shall ensure that appropriate data are determined, collected and analyzed to assess the suitability and effectiveness of the biorisk management system and to evaluate where continual improvement of the system can be made.

The organization should develop and implement methods to measure proactively and reactively, as appropriate, the effectiveness of its biorisk management programme and to determine if any improvements are required.

A system to measure and analyze data may include:

— identification of matrices appropriate for biorisk management, e.g. data from performance measurements from staff, equipment and training;

— results of the risk assessment analysis and controls;

— results of walk-through inspections and audits, both internal and external;

— reported accidents, injuries and near misses and the actions taken to prevent reoccurrence;

— quality control, performance results and calibration of the equipment (e.g. safety and security equipment and systems testing);

— environmental sampling;

— results of security and emergency response exercises;

— analysis of documentation and records (e.g. review of biological material inventories);

— employee surveys;

— unanticipated events which were not considered during the risk assessment, e.g. failure of equipment previously unknown or events in similar facilities; and

— response to non-conformances resulting from an inspection or a biorisk management system audit or job hazard assessments.

The analysis should include data generated as a result of monitoring, measurement, audits and analysis and from other sources. Such analysis should be conducted at least annually and more often if justified by the risks and the scope of operations. The results of the analysis should be applied in the management review.

The result of the above is that the facility has a risk based performance management system that analysis measures which support the biorisk management system. The data is used as a driver for needed change and continual improvement.

4.5.2 Records, document and data control

The organization shall ensure that records, documents and data are established, controlled and maintained to provide evidence of conformity to the requirements of this standard and that they remain legible, readily identifiable and retrievable.

The organization should establish a document control programme that will demonstrate that its biorisk management programme meets the requirements of the CWA 15793:2008.

Where appropriate, documents should be identified and controlled based upon the nature of the work and need for record keeping.

The list of controlled documents is neither exhaustive nor comprehensive but includes some of the main areas that should be formal and subject to document control. Data should be constructed as documents in this context. A procedure should be established to define the controls needed for the identification, storage, protection, retrieval, retention time and disposal of records. A procedure should be established to define the controls needed to approve documents prior to issue or public release to ensure sensitive information such as specific freezer locations of pathogen repositories is not inadvertently released. Procedures also should be established to define the controls for review, update and re-approval of documents, and for the change control and revision processes.

Controlled documents may include:

a) risk assessments, standard operating procedures (SOPs) and safety manuals;

b) job hazard analysis and charts of authority;

c) design records and commissioning / test plans, maintenance plans and records and all associated data;

d) audit and inspection checklists and reports;

e) laboratory biosecurity manuals and risk assessments, authorizations and other security documents;

f) training records;

g) containment equipment certifications

h) documentation related to equipment quality control records

i) inventories of receipt, storage, usage, shipping and disposal of biological materials;

j) consultation reports (internal and external);

k) accident / incident reports and follow up;

l) medical and health surveillance reports;

m) emergency response drills reports;

n) management review minutes;

o) non-conformity records and follow up; and

p) job descriptions.

For the process of document and data control and record retention, the organization should consider the following:

— a review of documentation and information needs, considering legal and other requirements related to documentation, data and record management;

— details of the documentation and information systems;

— a defined process for version control and documentation of the latest revision date or the next revision due date;

— assigning responsibility for documentation and maintenance of the information, including retention periods and disposal;

— deciding in what medium the information will be recorded and stored, considering issues related with electronic repositories (document versioning, electronic records, etc.);

— for electronic documentation and electronic keeping systems, software compatibility should be considered, especially when software upgrades are being implemented;

— deciding if information needs to be secured, and how it will be secured;

— assuring that information is accessible only to people who need it; and

— current documentation is sufficiently comprehensive to ensure that the biorisk management programme can be adequately understood and effectively and efficiently implemented.

The consequence is a comprehensive secured and easily accessible document and data control and management system that is current and provides evidence of conformity to the requirements of the standard and is easily available to all appropriate individuals.

4.5.3 Inventory monitoring and control

The organization shall ensure that a review of the inventory is conducted at predetermined intervals based on risk and at a level and frequency whereby materials can be accounted for in an appropriate manner.

The organization shall ensure that the measures are put in place to minimize the quantities of biological agents and toxins that make up the inventory.

The organization should ensure that the inventory is well maintained and reviewed on a regular basis and that no longer useful biological materials are destroyed*. The nature of the inventory and associated controls should be based upon the nature of the material held and the risk of harm should it be misplaced or removed with the intention of misuse. For many biological agents and toxins, the checks may be of a lower frequency*

and stringency than for others with greater potential for causing harm. Such measures may include numbered sequences of tubes, periodic inspections and crosschecks with records of materials held.

The organization should demonstrate proactive measures toward the reduction of risk through elimination, substitution or minimization of volumes / quantities of biological agents and toxins used, and the number of manipulations conducted.

Procedures should be in place to investigate potentially missing biological agents appropriate for the level of risk.

Components of an inventory management system may include:

— inventory that contains all biological agents and toxins in storage and in use at the facility;

— inventory control plan and mechanisms;

— the identity of the responsible personnel for review of the inventory;

— measures or systems of control (review) including tubes and box numbering, relevance of biomaterials in tubes with the list inventory;

— rationale for the minimising of the quantity of biological agents held by the organization (inventory control plan);

— a process for a periodic review of the inventory;

— protocols for investigating record discrepancies and tracing missing biological agents that are appropriate for the level of risk; and

— a well-defined system of audit or control of inventory.

The outcome is a functional and complete inventory that allows the organization to keep track of biological agents and toxins in the facility.

4.5.4 Accident and incident investigation, non-conformity, corrective and preventive actions

4.5.4.1 Accident / incident investigation

The organization shall establish and maintain documented procedures to define, record, analyze and learn from accidents and incidents involving biological agents and toxins.

Procedures should be set in place to ensure that what constitutes an accident or incident is clearly defined and communicated to all relevant personnel, and may include events of exposure and accidental release. Accidents and incidents provide an indication that the systems designed to manage biorisk may have failed, and it is essential that lessons are learned and improvements are made where possible.

The purpose of the procedure is to prevent further occurrences of the situation by identifying and dealing with the root cause(s) of the problem.

As a minimum, the accident / incident investigation process should include:

— *identifying those responsible for maintaining the accident / incident reporting system;*

— *defining what constitutes an accident / incident, and what triggers recording and reporting;*

— *specifying required documentation to support the system;*

— *identifying the reports that will be generated, their frequency and distribution;*

— *ensuring analysis of trends;*

— *identifying root causes using individuals trained in investigation techniques;*

— *providing feedback at regular intervals and action tracking mechanisms to ensure that lessons learned result in action to avoid the repeat of such events and / or minimize their potential impact;*

— *identifying where it may be appropriate or necessary for security professionals may be required to coordinate with law enforcement; and*

— management should participate in investigations of major events.

The investigative process should be well documented to help improve systems at the facility. The process for accident and incident investigation should make use of available data such as:

— risk assessments;

— standard operating procedures (SOPs);

— emergency plans;

— accident reports, interviews of relevant people;

— inspections; and

— staff training records.

The result of the above inputs should be:

— a well defined and implemented incident and accident investigation procedure designed to identify root causes of incidents and accidents and reduce those incidents and accidents and the risk to workers; and

— a documented investigation report and an analysis of the effectiveness of the programme.

4.5.4.2 Control of nonconformities

The organization shall ensure that situations that do not conform to the requirements of this standard are identified and controlled to prevent undesirable consequences. Records of the nature of the non-conformity and any subsequent action taken shall be maintained.

The controls and related responsibilities and authorities for dealing with non-conforming situations should be defined in a procedure.

A systematic approach is necessary for the ongoing effectiveness of the biorisk management system to address nonconformities. The approach should include:

— procedures to identify, investigate and correct nonconformities taking into account audit and inspection reports, root cause analysis of nonconformities identified;

— reviews of operations to prevent anticipated re-occurrence;

— analysis of the impact of the nonconformity on other aspects of the biorisk management and correction of potential effects;

— revision of the biorisk management and documentation of the changes made;

— communication of relevant nonconformities and corrective and preventive actions to impacted individuals; and

— addressing responsibilities, authority, and the steps to the process.

The result should be the establishment of a mechanism to identify nonconformities and take action to control and prevent them from re-occurrence.

4.5.4.3 Corrective action

The organization shall ensure action is taken to eliminate the causes of non-conformities with the requirements of this standard in order to prevent recurrence. Corrective actions shall be appropriate to the effects of the nonconformities encountered.

The organization should design a programme for the review and elimination of potential causes of nonconformities and prevent their reoccurrence.

A procedure should be established to define requirements for:

a) reviewing the non-conformities;

b) determining the cause of non-conformities;

c) evaluating the need for action to ensure that non-conformities do not recur;

d) determining and implementing action needed;

e) recording results of action taken;

f) reviewing corrective actions taken.

Elements of a corrective action plan may include:

— reports and recommendations of inspections and reviews, audits;

— accidents and incidents investigations;

— identification, prioritisation, and implementation of corrective measures; and

— evaluation of risk assessment results.

The above should produce a programme that demonstrates the effective and timely control measures for nonconformities.

4.5.4.4 Preventive action

The organization shall ensure action is taken to identify and eliminate the causes of potential non-conformities in order to prevent their occurrence. Preventive actions shall be appropriate to the effects of the potential nonconformities.

The facility should have an established preventative programme aimed at eliminating the root causes of potential nonconformities. Preventive action is generally based on reported incidents, or near-misses, or changes in the facility that may affect the biorisk management programme.

A procedure should be established to define requirements for:

a) determining the potential non-conformities and their causes;

b) evaluating the need for action to prevent occurrence of non-conformities;

c) determining and implementing routine *action needed* (e.g. equipment QC, personnel training)*;*

d) recording of the results of action taken; and

e) continuously *reviewing preventive action taken.*

A preventive procedure should take into consideration:

— reported accidents, incidents and near-misses and their investigation records;

— changes in the facility that may affect the biorisk management programme;

— audit, inspection and walk-through reports;

— results of medical surveillance and preventative medical programmes;

— results of periodic personnel and facility reviews and advice from employees; and

— equipment malfunctions.

The result will be a proactive programme to optimize the effectiveness of the biorisk management programme based on identified nonconformities.

4.5.5 Inspection and audit

The organization shall ensure that a programme of inspection and audit is conducted which is appropriate to the risk associated with the facility.

Inspections and audits shall be conducted at planned intervals to determine if the biorisk management system conforms to the documented plans and to the requirements of this standard, and that it is effectively implemented and maintained.

Management responsible for the area being inspected / audited shall ensure that any actions are taken without undue delay to eliminate detected non-conformities and their causes. Follow-up activities arising shall include the verification of the actions taken and the reporting of verification results.

The organization should establish a formal assessment process to review and evaluate the conformity and effectiveness of their biorisk management programme. This programme may include internal audits and inspections, as well as third-party external audits.

Inspections may be frequent checks on specific areas conducted to ensure sufficient standards are being maintained (e.g. disinfectant levels / concentrations and air exchange rates / maintenance of directional air flow) or more extensive but less frequent inspections of laboratories, facilities or other operations. Random, unannounced inspections and inventory audits can help ensure compliance at all times, not just in time for scheduled inspections. Audits should be performed by competent individuals who are independent of the activity being audited. Records should be maintained of findings of inspections / audits, including action taken to close out any non-conformities or improvement opportunities.

Audits and inspections should be undertaken by competent personnel. Individuals conducting inspections and audits should have knowledge and experience in the biorisk management systems, the organization's operations and the scope of work and general facility design within the operational legal framework.

The terms "Audit" and "Inspection" are defined in CWA 15793:2008.

An inspection and audit programme may include:

— reports from internal and external audits, inspections and management system reviews;

— informal physical inspections of work areas;

— inventory audits (announced and unannounced);

— document reviews;

— results of self-assessments;

— incident and accident reports;

— routine or random equipment performance evaluations; and

— routine or random facility systems evaluations or recertification, e.g. HVAC (heating, ventilating and air conditioning) system and airflow analysis, filter system integrity reviews.

An audit and inspection programme should consider the following:

— the scope of audit or inspection (typically, a written charge or scope document would be useful);

— the team performing the audit should have defined roles and responsibilities and be selected through an agreed, documented process;

— agreement on the procedure for audits / inspections which may include check-lists, and written scope;

— relevant personnel should be interviewed; determine if all personnel will be subject to interviews;

— relevant documentation should be examined; determine which are these documents (e.g. policy, objectives, emergency procedures, permits, training records, etc. depending on the described scope);

— agreement on how results of the inspection or audit will be measured and reported and who would receive the report;

— agreement on the frequency of audits based on the facility's risk (determined by risk assessment); additional audits may be conducted after an incident; and

— whether unannounced audits and inspections may be performed under specific circumstances.

Corrective action plans, implementation timelines and any follow-up actions should be developed and incorporated in the report.

Typical result may include an inspection and audit programme that, depending on the scope, develops a clear concise report detailing the identification of nonconformities:

— documentation about the audit and auditing team;

— assessments of the effectiveness of biorisk management procedures and practices;

— detailed assessments of levels of compliance with procedures and practices; and

— corrective procedures where nonconformities are identified by the audit.

The report should be documented and shared with relevant personnel, as appropriate.

4.6 Review

4.6.1 Biorisk management review

Top management shall review the organization's biorisk management system at planned intervals, to ensure its continuing suitability, adequacy and effectiveness. The review shall include assessing opportunities for improvement and the need for changes to the system, procedures, policies and objectives. Records from the management review shall be maintained.

Top management should establish a programme for periodic review of the biorisk management system, to assess its implementation, to ensure it remains appropriate and suitable for achieving the organization's biorisk management policies and objectives, and consider any appropriate changes.

The management review should be conducted at a defined frequency determined by the needs of the organization, but at least annually.

The biorisk management review process should be documented to describe:

— frequency, based upon risk (typically, a best practice may be at least annually);

— topics to be addressed;

— who will participate in the review and who will receive the completed review;

— roles and responsibilities in relation to the review; and

— expected outcome.

The topics addressed during the review may include:

— adequacy of the current biorisk policy;

— goals and objectives to determine any needs for modification or need to establish new ones;

— adequacy of the risk assessment system, including levels of risk and control measures;

— adequacy of resources (financial, people, materials, physical facilities);

— effectiveness of inspection process;

— effectiveness of the hazard reporting process;

— data related to accidents / incidents;

— effectiveness of SOPs;

— results of the audits and inspections;

— effectiveness of the corrective and preventive actions;

— preparedness of the organization to deal with emergencies; and

— assessment of the effects of foreseeable changes to operations, resources (e.g. human, material, financial), legislation or technology.

The management review may be divided into components that are conducted at different time intervals during the defined period. However, the results of the partial reviews should be combined to create an overall view of the suitability, adequacy and effectiveness of the management system.

The review input should include information on:

— *results of audits;*

— *compliance to SOPs and work instructions;*

— *status of risk assessment activities;*

— *status of preventive and corrective actions;*

— *follow-up actions from previous management reviews;*

— *changes that could affect the system;*

— *recommendations for improvement; and*

— *results of accident / incident investigations.*

The review output should include decisions and actions related to:

— *improvement of the effectiveness of the biorisk management system;*

— *improvement related to the requirements and risk assessments; and*

— *resource needs.*

Bibliography

[1] CWA 16335:2011, Biosafety professional competence

[2] ILO-OSH 2001, Guidelines on occupational safety and health management systems

[3] ISO 9001:2008, Quality management systems – Requirements

[4] ISO 14001:2004, Environmental managements systems – Requirements with guidance for use

[5] ISO/IEC 17025:2005, General requirements for the competence of testing and calibration laboratories

[6] ISO/IEC 27001:2005, Information technology – Security techniques – Information security management systems - Requirements

[7] ISO 22000:2005, Food safety management systems – Requirements for any organization in the food chain

[8] ISO/IEC 20000, Information technology – Service management

[9] ISO 15189:2007, Medical laboratories – Particular requirements for quality and competence

[10] National Sanitation Foundation Code No.49, Biological Safety Cabinets

[11] OHSAS 18001:2007, Occupational health and safety management systems – Requirements

[12] PAS 99:2006, Specification of common management systems requirements as a framework for integration