

SAND2012-6385C

# Biosafety and Biosecurity

10 August 2012



# Objectives

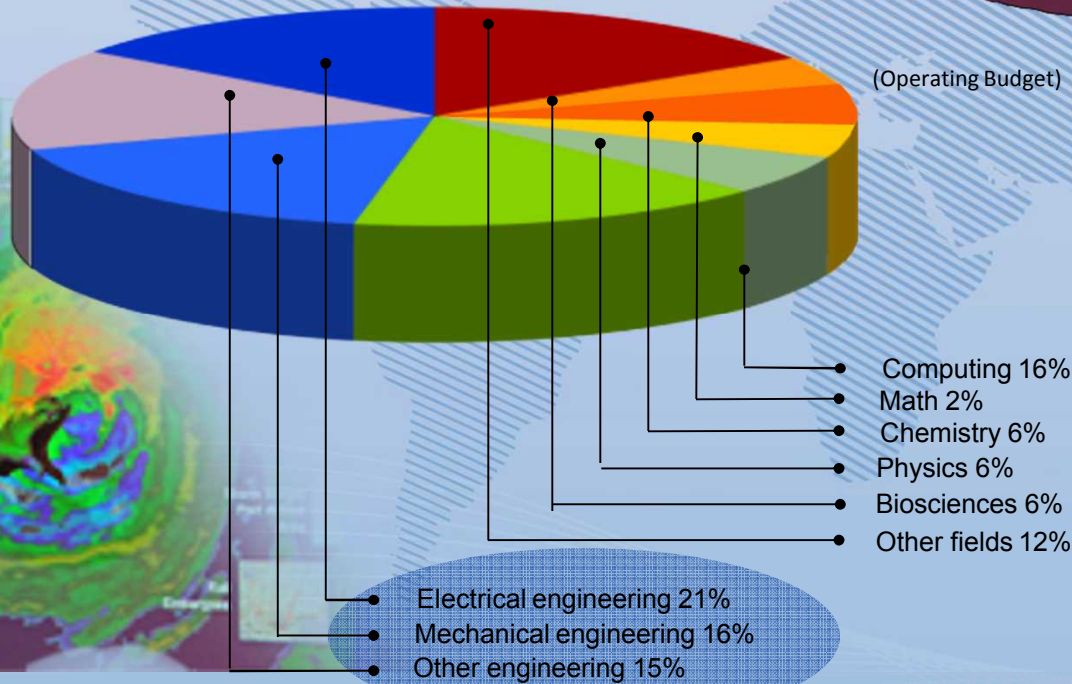
---

- Introduce Sandia National Laboratories, a key CBEP partner
- What is Biosafety and Biosecurity and why is it important
- Present the AMP model of Biorisk Management
- Learn about the five pillars of Biosecurity

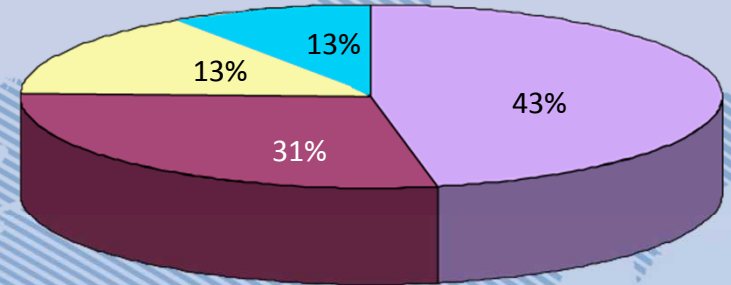
# People and Budget (As of October 15, 2010)

- On-site workforce: 11,677
- Regular employees: 8,607
- Gross payroll: ~\$898.7 million

Technical staff (4,277) by discipline:

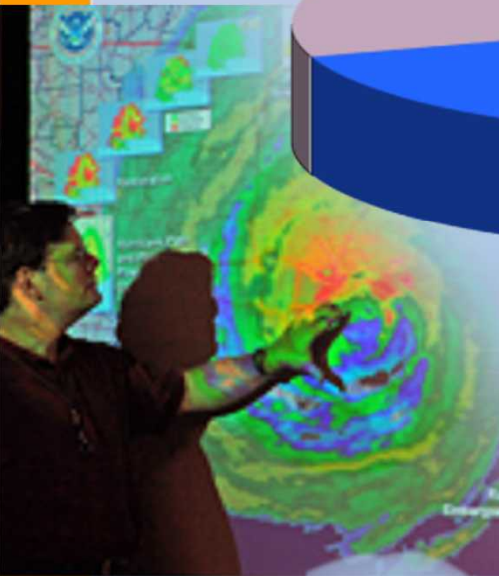


FY10 operating revenue  
\$2.3 billion



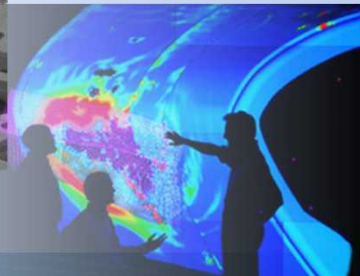
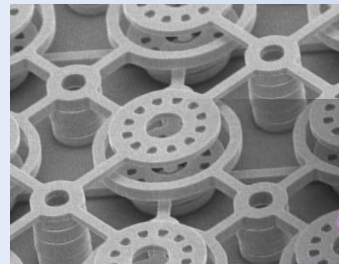
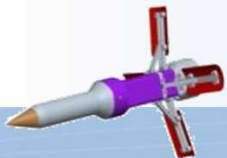
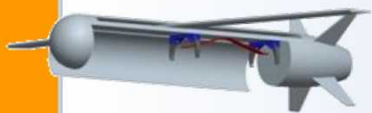
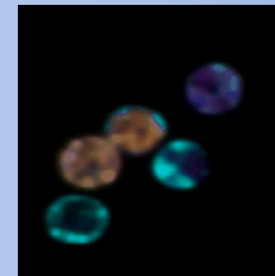
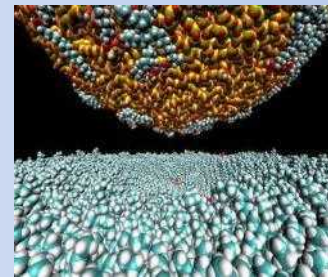
(Operating Budget)

- Nuclear Weapons
- Defense Systems & Assessments
- Energy, Climate, & Infrastructure Security
- International, Homeland, and Nuclear Security



# SNL Research and Capabilities

- SNL Programmatic Areas
  - Nuclear Weapons
  - Defense Systems and Assessments
  - Energy, Climate, and Infrastructure Security
  - International, Homeland, and Nuclear Security
- SNL Research Areas
  - Computer science
  - Materials
  - Engineering sciences
  - Microelectronics
  - Bioscience
  - Pulsed Power



# SNL International, Homeland, and Nuclear Security

## Program Areas

- Critical Asset Protection
- Global Security
- Homeland Defense and Force Protection
- Homeland Security

## Areas of Expertise

- Countering Bioterrorism
- Nuclear, Radiological, and Chemical Risk Reduction
- Nonproliferation and Arms Control
- Physical Security
- Emergency Response
- Systems Analysis and Engineering
- Border Security
- Aviation and Airworthiness Security



## AWARENESS – PREVENTION

Technical analysis and global engagement to recognize threats and risks, and to promote responsible work in the life sciences



## PREPAREDNESS - DETECTION

Systems for diagnosing biological incidents early and identifying their sources



## RESPONSE – RECOVERY

Technology and methods for agent characterization, consequence management, and environmental restoration



“ Science, technology, and technical policy solutions for reducing biological threats around the world. ”

# International Biological Threat Reduction

## *Innovative solutions for countering biological threats globally*

- Promote the responsible use of biological agents, equipment, and expertise globally.
- Strengthen capacities to safely, securely, and responsibly detect, handle, and control dangerous biological agents.
- Improve understanding and management of the risks associated with accidental and deliberate misuse of biological agents.



# IBTR Core Capabilities

- **Laboratory biorisk management**
  - Biorisk management standards and regulatory frameworks
  - Core biorisk management program documents
  - Lab design / programming expertise
  - Facility specific biosafety and biosecurity threat, vulnerability, and risk assessments
  - Biorisk (biosafety and biosecurity) upgrades
- **Biothreat identification and analysis**
  - Global analysis
  - Country and regional analyses
- **Capacity building and outreach**
  - Biorisk management training
  - Training centers
  - Law enforcement
- **Building inherently safer and more secure capabilities**
  - Surveillance and control
  - Public and vet health
  - Incident detection and response





# **GBRMC = Global Biorisk Management Curriculum**

## **Mission**

- Biosafety & Biosecurity training materials. . .
  - Strategic
  - Sustainable
  - Anywhere, anytime
  - Well-branded
  - Well-managed
  - Customizable

# Strategic & Sustainable Biorisk Management



# Global Biorisk Curriculum Library examples

## Basic Track

*Audience: all personnel involved in biorisk management*

- Biorisk Management Basics
  - Orientation to biorisk management
  - Bioethics
  - Dual-use and responsible conduct of research
  - Risk Characterization & Evaluation
  - Biosafety Risk Assessment
  - Biosecurity Risk Assessment
  - Biorisk Mitigation Strategies
  - Introduction to Incident Management & Response

## Laboratory-Level Track

*Audience: Biorisk Management Advisors, Scientific/Laboratory Management, Lab Workforce*

- Lab-Level Administrative Controls
  - Human Performance for Biorisk Management in the Laboratory
  - Developing, evaluating, validating, and communicating standard operating procedures
  - Laboratory level hazard and risk communication

## Laboratory-Level Track, continued

- Lab-Level Operational Controls
  - Risk mitigation strategies
  - Developing, evaluating, validating, and communicating standard operating procedures
  - Facility features
  - Engineering Controls and Equipment
  - Good laboratory practices
  - Personal protective equipment
  - Decontamination
  - Disposal
  - Biosecurity
  - Field biosecurity
  - Shipping Infectious Substances and Biological Specimens
- Reporting, monitoring, and Response
  - Incident recognition and response in the laboratory
  - Drills, audits, and inspections (lab-level)



# Global Biorisk Curriculum Library examples

## Management & Leadership Track

*Audience: (Policy Makers) Top Management, Biorisk Management Advisors, Scientific/Laboratory Management*

- Policy, Planning, and Assessment
  - Writing and communicating biorisk management policy
  - Establishing and communicating BRM roles, responsibilities, objectives, and goals
  - Developing, conducting, and maintaining a hazard inventory
  - Identifying legal requirements that impact BRM
  - Work program review and approval
- Developing and Maintaining Human Capacity for Biorisk Management (Managing People)
  - Managing human performance in the BRM workforce
  - Developing, implementing, and evaluating training and other methods to assure BRM competence
  - Establishing and maintaining formal and informal BRM mentoring programs
  - Establishing and maintaining Worker Health Programs
  - Developing roles & responsibilities for risk-based access to and accountability for biological agents and toxins

## Management & Leadership Track, continued

- Developing and Maintaining Physical Infrastructure for Biorisk Management
  - Understanding and maintaining facilities & equipment for biorisk management
  - Basic features & maintenance for physical and information security measures
- Incident Management & Response
  - Incident Response Planning and Preparation
  - Incident Response & Investigation
  - Incident Response Evaluation & Improvement
- Measuring and Improving Biorisk Management Performance
  - Measurement and Analysis of Biorisk Management System Performance
  - Conducting Audits and Inspections to Assess Biorisk Management Performance
  - Revising and Improving a Biorisk Management System based on Performance Results
  - Establishing and Using Performance Indicators

# IBTR's Global Experience



# SNL Conclusions

---

- **Sandia is a US Government National Laboratory**
  - FFRDC status (“quasi-government”)
  - Mission to provide technical advice and support on national security issues to USG
- **Sponsors can tap into the entirety of Sandia, such as:**
  - Disease detection, microfluidics for medical diagnostics, bioinformatics
  - Security specialists
  - Systems analysis
  - Bioforensics, environmental restoration
  - International nuclear nonproliferation experience
- **IBTR has 10+ years of global collaborative biothreat reduction experience**
  - Multi-disciplinary team
- **SNL has infrastructure for international engagement**
  - International business services
  - International programs building, including training, technology, and demonstrations area
  - Demonstrated ability to work in high and extreme risk countries
    - *Host visiting scholars at Sandia and/or meet in 3<sup>rd</sup> party countries to advance projects*
    - *Extensive global travel experience*

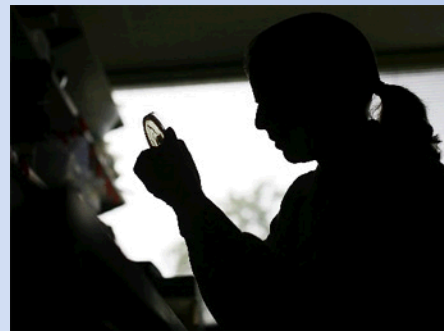
# Key IBTR Partners



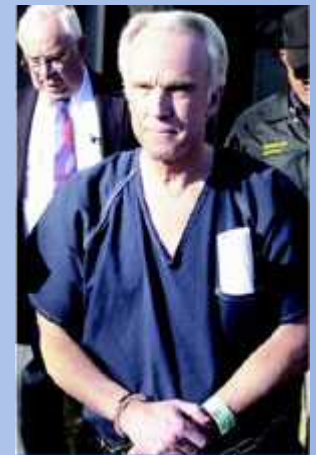


# Examples of Safety and Security Issues Arising from Problems in Biorisk Management

- Texas A&M University, United States, 2006 – 2007
  - U.S. federal officials suspend all Select Agent research due to failures to report two incidents
- Pirbright Laboratory, Institute of Animal Health, United Kingdom, 2007
  - Leaks from pipes in the effluent system caused Foot and Mouth Disease outbreak
  - Pipes were known to need maintenance
- Professor Thomas Butler, United States, 2003
  - 30 vials of *Yersinia pestis* missing from lab (never recovered); Butler served 19 months in jail
- Laboratory-acquired outbreaks of SARS, 2003 – 2004
  - Singapore—September 2003
  - Taiwan (China)—December 2003
  - Beijing and Anhui (China)—March 2004



TAMU Select Agent researcher  
– Dallas Morning News



Thomas Butler

# Bioterrorism Examples

- Rajneeshees – 1984
  - Contaminated restaurant salad bars in The Dalles, Oregon with salmonella spp. bacteria



*Bhagwan  
Shree  
Rajneesh*



*Aerosolization of *Bacillus anthracis* and botulinum toxin by Aum Shinrikyo*

- **Aum Shinrikyo – 1990s**
  - Aerosolized and disseminated biological agents in Tokyo
    - Vaccine strain of *Bacillus anthracis*
    - Inactive strain of *Clostridium botulinum*

# Illustrative Case:

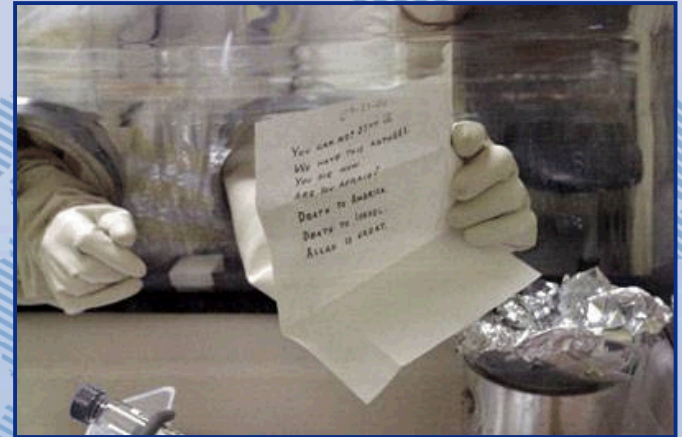
## Diane Thompson, October 1996

- Location: Hospital in Dallas, TX
- Perpetrator: Diane Thompson
  - Clinical laboratory technician
- Objective:
  - Unclear, possibly revenge against former boyfriend and cover-up by infecting co-workers
- Organism:
  - *Shigella dysenteriae* Type 2
  - Acquired from clinical laboratory of the St. Paul Medical Center where she worked
- Dissemination
  - Contaminated pastries in the office break room
  - Infected 12 of her coworkers
- Outcome
  - Arrested, convicted, 20 year sentence



# Illustrative Case: Anthrax, October 2001

- Location: More than 60 sites in the US
- Perpetrator: FBI names Bruce Ivins
- Objective: Unknown
- Organism:
  - *Bacillus anthracis*
- Dissemination
  - 7 letters sent through postal system
  - 22 confirmed cases of anthrax
    - 11 Cutaneous
    - 11 Inhalational (5 Deaths)
- Outcome:
  - FBI unveils evidence against Ivins

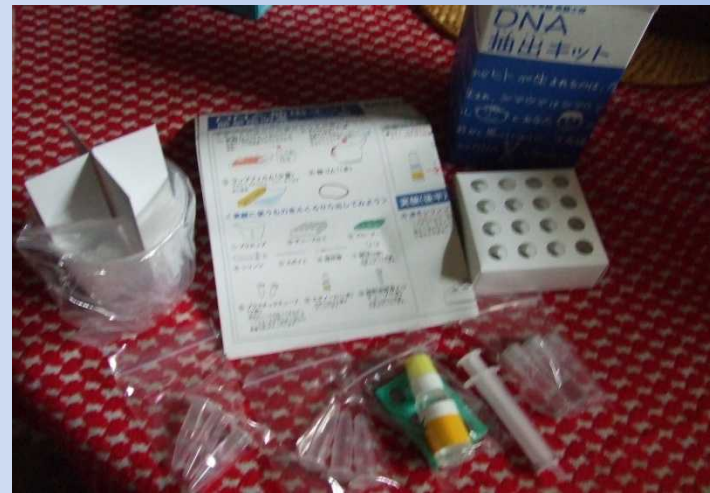


ANTHRAX INVESTIGATION

**FBI Discusses Microbial Forensics—  
But Key Questions Remain Unanswered**

# Nature of Biology is Changing

- Rapid technological advances
- Technologies becoming more available
  - Geographically
  - Individuals



DNA extraction kit for 10 year old kids, sold by Japanese National Museum of Emerging Science and Innovation

# BW is Different Than Other WMD

- Naturally-occurring
    - With only a few notable exceptions:
      - Variola major virus
      - 1918 Influenza virus
  - Dual-use
    - Materials
    - Technologies
    - Expertise
  - Wide variety of materials
    - Deadly to incapacitating
    - Human, animal, zoonotic, plant
  - Self-replicating
    - Minute quantities of concern
  - Not detectable at a distance
- Present in many types of facilities
    - Research laboratories, clinical laboratories, hospitals
    - Private and public sector
  - Present at multiple locations within a facility
    - In laboratory, in storage, in animals, in waste stream
  - Synthetic biology
    - De-novo synthesis
    - Turning non-pathogenic material into virulent organism

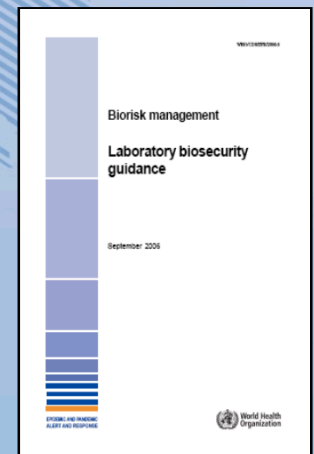
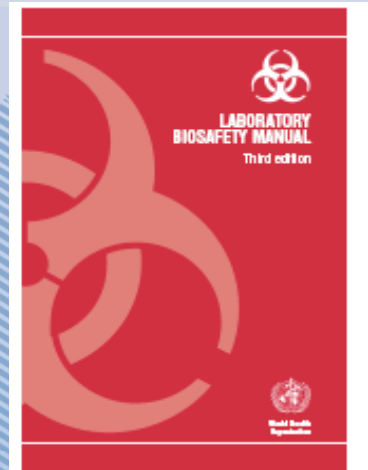
Source: Jonathan B. Tucker, "Biosecurity: Limiting Terrorist Access to Deadly Pathogens," Peaceworks No. 52, United States Institute of Peace, November 2003.

# Biorisk Management

- How can these risks be addressed?
- **Biorisk management** is a new discipline that specializes in the assessment and mitigation of biorisks
  - Biosafety
  - Biosecurity

# Definitions

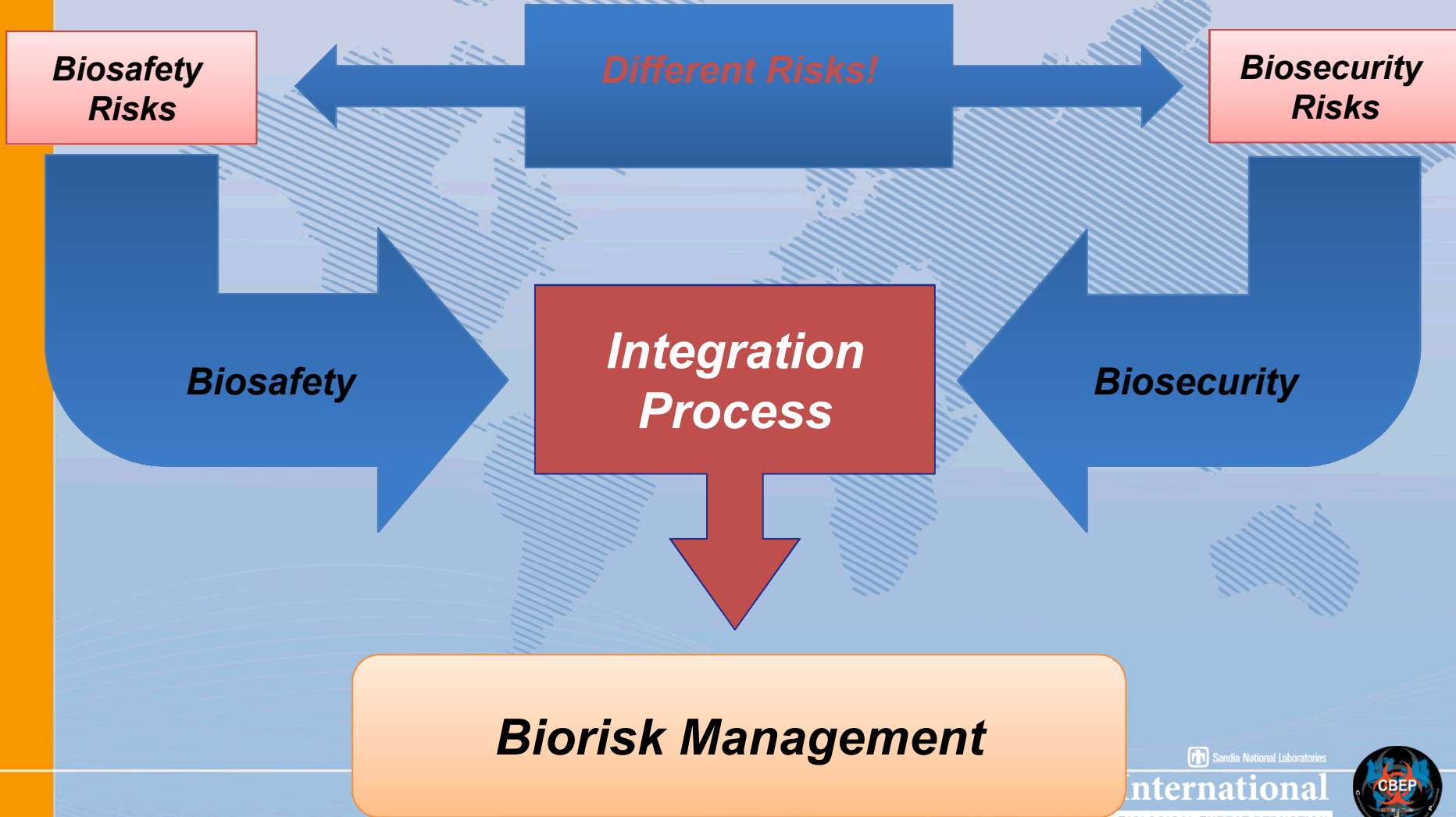
- **Biosafety:** containment principles, technologies, and practices implemented to prevent unintentional exposure to pathogens and toxins, or their unintentional release<sup>1</sup>
- **Biosecurity:** protection, control and accountability for valuable biological materials within laboratories, in order to prevent their unauthorized access, loss, theft, misuse, diversion or intentional release.<sup>2</sup>



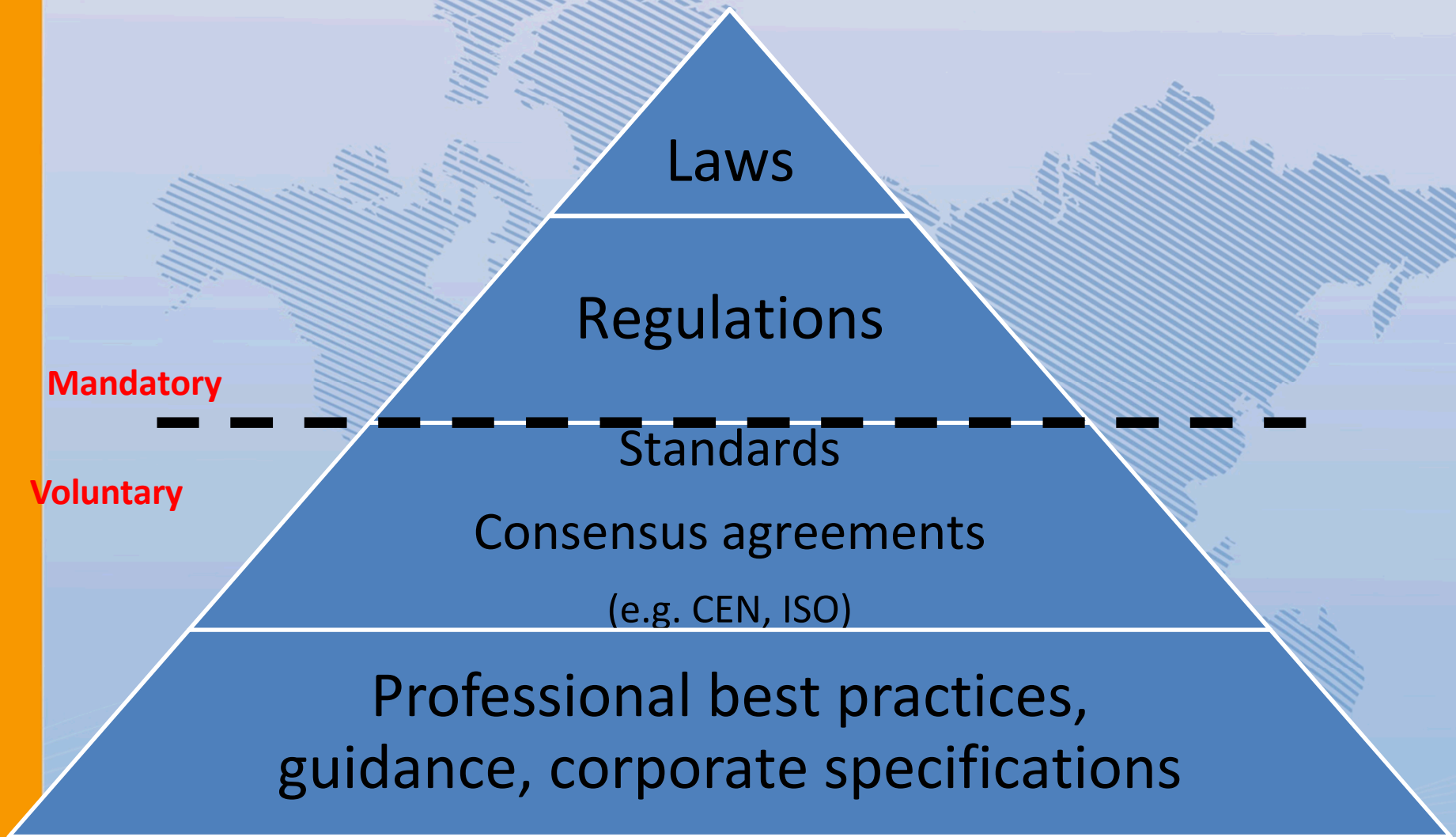
<sup>1</sup>Laboratory biosafety manual, Third edition (World Health Organization, 2004)

<sup>2</sup> Biorisk management - Laboratory biosecurity guidance (World Health Organization, 2006)

# Biosafety and Biosecurity Integration



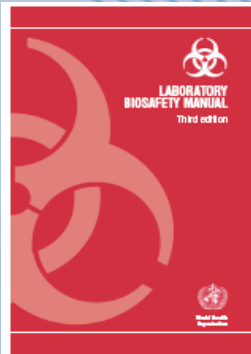
# Standards, Regulations, Best Practice



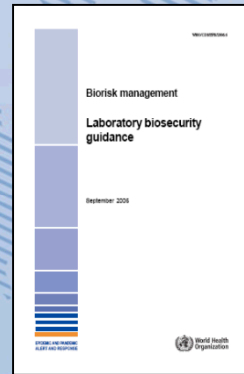
# Selected Key International Documents

World Health Organization (WHO)

European Committee for Standardization (CEN)



**2004** – Laboratory Biosafety Manual, 3<sup>rd</sup> Edition (WHO)



**2006** – Biorisk Management: Laboratory Biosecurity Guidance (WHO/FAO/OIE)

*Technical guidance*



**2008** – CWA 15793:2008 – Laboratory biorisk management standard (CEN)

**2011** – CWA 16335:2011 – Biosafety Professional Competence (CEN)

**2012** – CWA 15793 Guidance Document

# Biorisk Management: The **AMP** Model

**Biorisk Management =  
Assessment, Mitigation, Performance**

# Key Components of Biorisk Management

## Biorisk **Assessment**

- Process of identifying the hazards and evaluating the risks associated with biological agents and toxins, taking into account the adequacy of any existing controls, and deciding whether or not the risks are acceptable

# Key Components of Biorisk Management

## Biorisk Mitigation

- Actions and control measures that are put into place to reduce or eliminate the risks associated with biological agents and toxins



# Key Components of Biorisk Management

## Performance

- The implementation of the entire biorisk management system, including evaluating and ensuring that the system is working the way it was designed. Another aspect of performance is the process of continually improving the system.

# Introduction to Biosafety Risk Assessment

A **biosafety risk assessment** is an analytical procedure designed to characterize and evaluate **safety** risks in a laboratory.



# Introduction to Biosafety Risk Assessment

A **biosafety risk assessment** allows a laboratory to determine the relative level of risk its different activities pose, and helps guide **risk mitigation decisions** so these are targeted to the most important risk.



# Risk Assessment

Think about this question:

*Is conducting a risk assessment simple? Why or why not?*



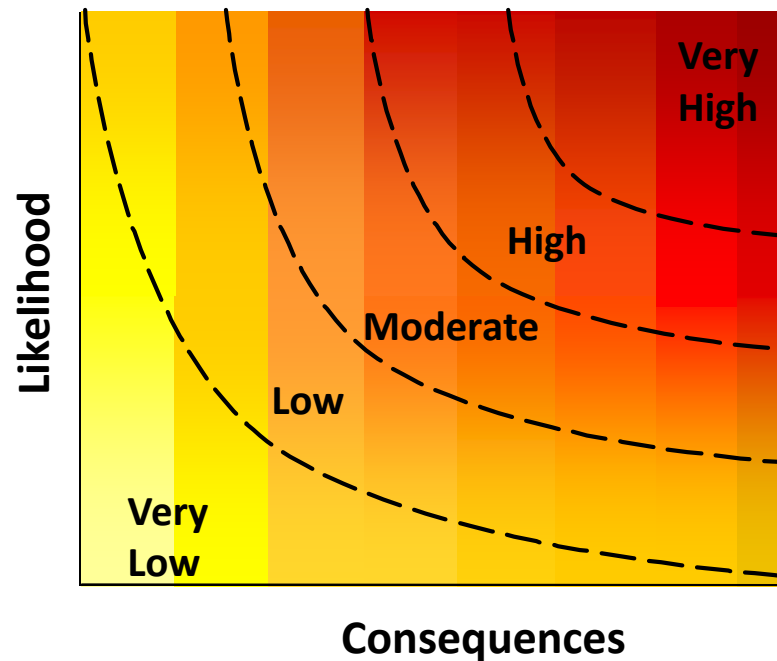
# What is the **risk** of crossing the road?



# Risk Assessment

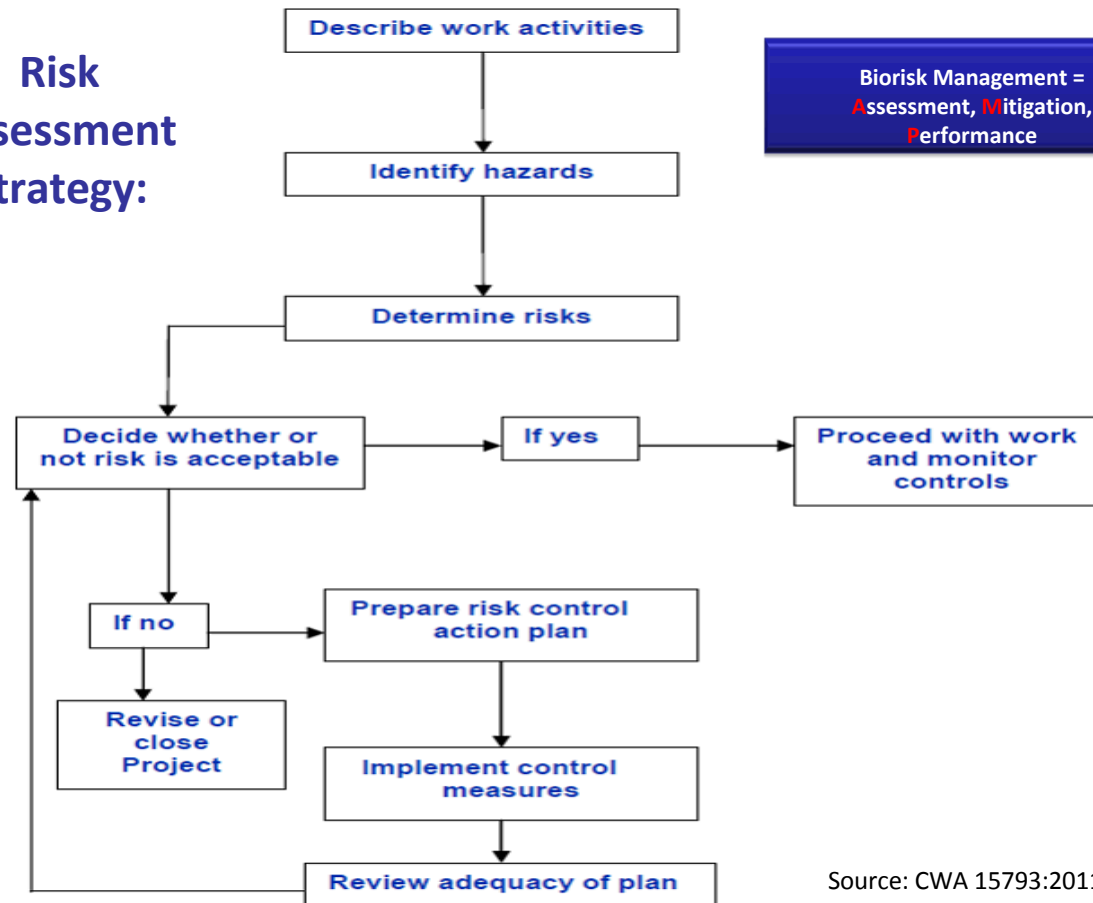
Risk is a function of **likelihood** and **consequences**

$$\text{Risk} = f(\text{Likelihood}, \text{Consequences})$$



# Risk Assessment Strategy

## Risk Assessment Strategy:



Source: CWA 15793:2011

# BioRAM

One available tool to aid in the laboratory risk assessment process is the **Biosafety and Biosecurity RAM (BioRAM)**.

**BioRAM** is a computerized **risk assessment tool** developed by Sandia National Laboratories, in partnership with the international community, to facilitate laboratory **biosafety and biosecurity risk assessments** by simplifying **risk characterization**.

# BioRAM

---

**BioRAM** uses only one of several possible risk assessment methodologies.

It is based on the input of biosafety experts and validated around the world. The **BioRAM** tool helps determine *relative* risk levels in a **comparable** and **repeatable** way.

<http://biosecurity.sandia.gov/BioRAM/>

# Risk Mitigation

## Now we will discuss Risk Mitigation

### Biorisk **Mitigation**

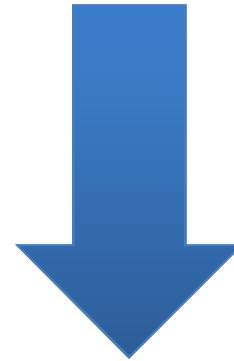
- Actions and control measures that are put into place to reduce or eliminate the risks associated with biological agents and toxins

**Question:** Why would we want our Risk Mitigation to be based on a proper Risk Assessment?

# Hierarchy of Controls

## Hierarchy of Controls

- ***Elimination or Substitution***
- **Engineering Controls**
- **Administrative Control**
- **Practices and Procedures**
- **Personal Protective Equipment**



Control methods at the top of the list are in general more effective and protective than those at the bottom, but this is not always the case.

# Mitigation Control Measures

**Elimination or Substitution:** Removing the hazard, not working with the agent or replacing the hazard with something less dangerous



# Engineering Controls

**Engineering controls** are physical changes to work stations, equipment, materials, production facilities, or any other relevant aspect of the work environment that reduce or prevent exposure to hazards

## Examples:

- **Primary Containment**
  - BSC
  - Sealable Containers including rotor cups
  - Cages
- **Secondary Containment**
  - Facility layout and construction
  - Airflow
  - Doors (with locks and access controls)
  - Sealable rooms
- **Waste**
  - Autoclave/Incinerator
  - Sharps Container



# Administrative and Procedural Controls

**Administrative controls** are policies, standards and guidelines used to control risks.

**Procedural controls** are processes and activities that have been shown in practice to be effective in reducing risks.

## Examples:

- **Good Lab Practices**

- No eating or drinking /No mouth pipetting
- Hand washing
- Spill cleaning / standard cleaning
- Sharps handling
- Aerosol prevention
- Inventory; Material Control and Accountability
- Documentation
- Waste handling
- Entry and Exit procedures

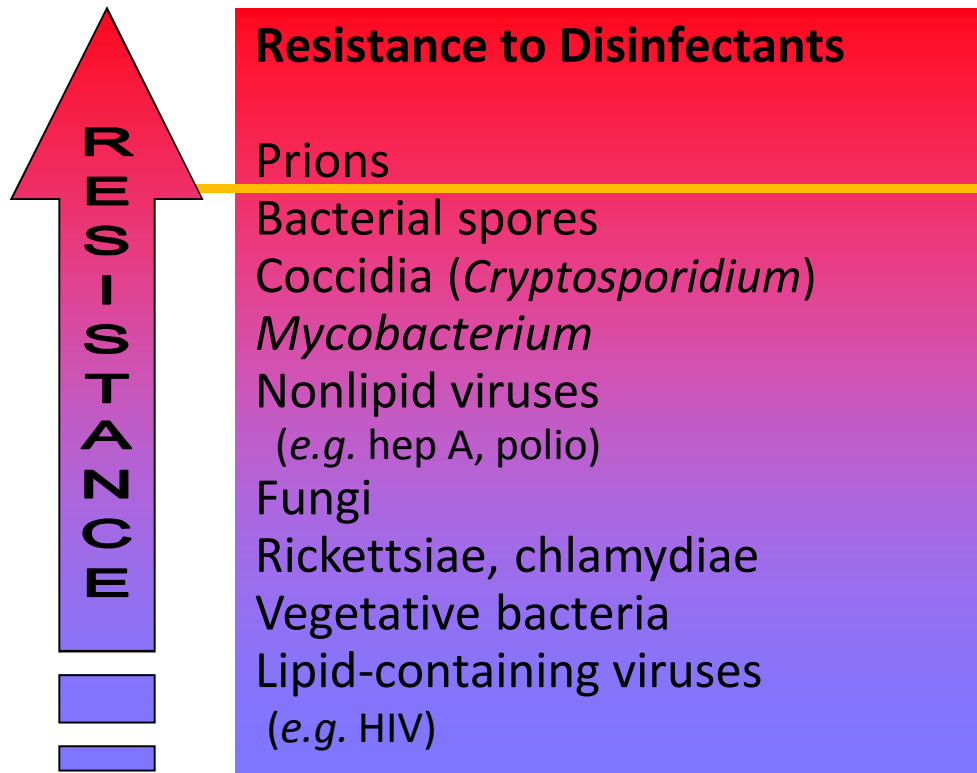
- **Personnel Management**

- Training
- Integrity verification
- Medical clearance

# Administrative and Procedural Controls

**Example** of the need for a proper risk assessment leading to proper mitigation:

*Disinfectants* need to be appropriate for the biological agent in use



# Administrative and Procedural Controls

## Example: Laboratory Waste Handling

### Laboratory wastes that may need decontamination include...

- **Solid, non-sharp waste, such as...**
  - Plastic labware (flasks, tubes, plates, bottles, vials)
  - Tissue or carcass waste (pathological)
- **Liquids, such as...**
  - Aspirates, culture fluids, rinses, washes, etc.
  - Sera, body fluids
- **Sharps, such as...**
  - Anything with a point or edge capable of piercing or cutting human skin
  - Glass labware (sometimes also broken plastic)

**It all depends on what organisms are being used and in what manner they are being used... ie all depends on the Risk Assessment**



Sandia National Laboratories

# Administrative and Procedural Controls

## Example: Material Control and Accountability

### For moderate risk biological agents

- Seed stocks cataloged and records stored securely
  - Transfers in and out
  - Source
  - Strain
  - Form
  - Responsible individual
- Working stocks, including infected animal status, tracked through laboratory notebooks



### For high risk biological agents

- Moderate plus
  - Increased control over working stocks

**It all depends on what organisms are being used and in what manner they are being used... i.e. all depends on the Risk Assessment**

# Standard Operating Procedures

## Standard Operating Procedures (SOPs)

- Written instructions that document a routine or repetitive activity
- Detail of processes necessary to perform a job safely and properly
- Describe both technical and administrative practices and operations
- Specific to an organization or laboratory

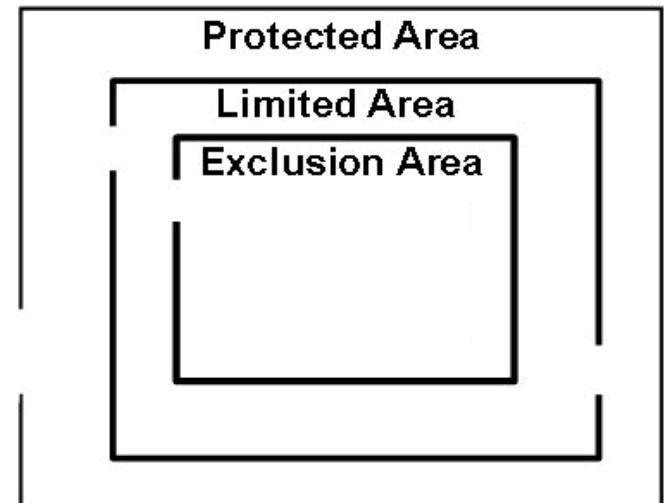


# Biosecurity Engineering and Procedural Controls

**Example:** Concept of **Graded Protection in Risk Management**, as applied to **Security**

- **Property Protection Areas**
  - Low risk assets
    - **Grounds**
    - **Public access offices**
    - **Warehouses**
- **Limited Areas**
  - Moderate risk assets
    - **Laboratories**
    - **Sensitive or administration offices**
    - **Hallways surrounding Exclusion Areas**
- **Exclusion Areas**
  - High risk assets
    - **High containment laboratories**
    - **Computer network hubs**

## Concentric Layers of Security



**Question:** Why is concentric good?

**Question:** How would you apply both engineering and procedural controls in lab biosecurity?

# Personal Protective Equipment (PPE)

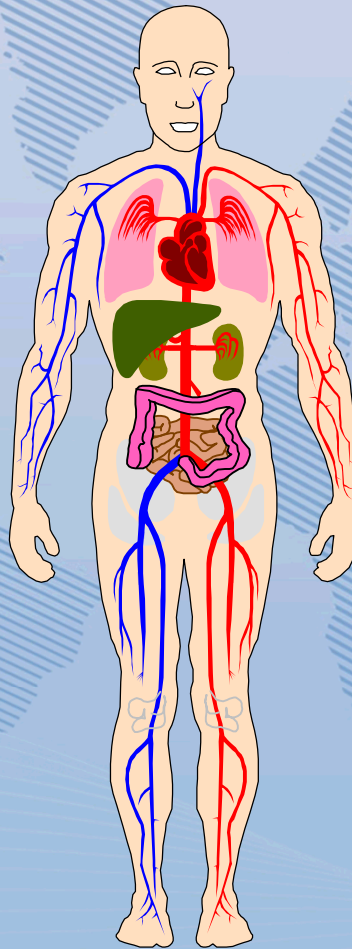
**Personal Protective Equipment** is a set of devices worn by the worker to protect against hazards in the laboratory.

## Examples:

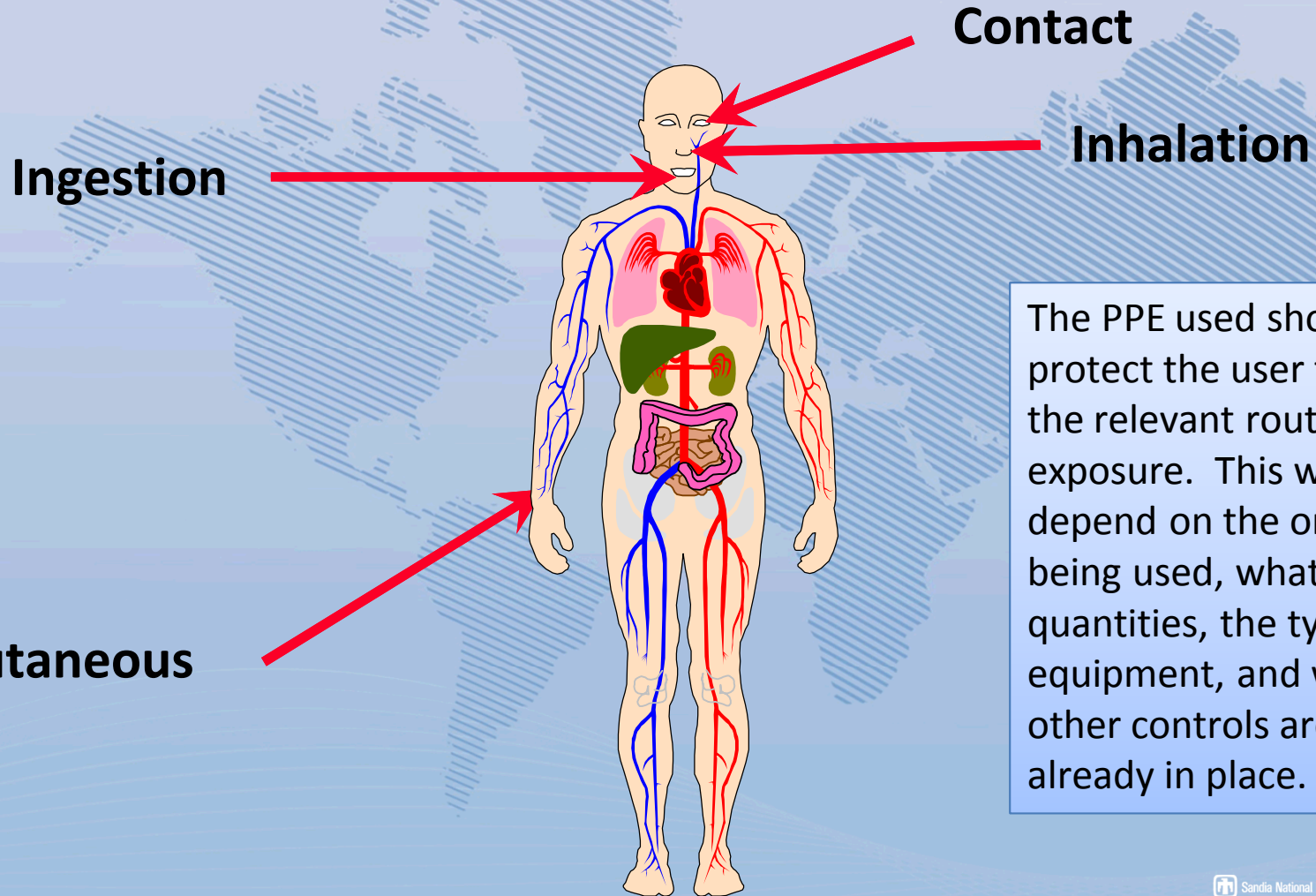
- Respiratory Protection and Fit
- Gloves
- Body cover
- Feet cover
- Eyewear
- Face cover



# Routes of Exposure



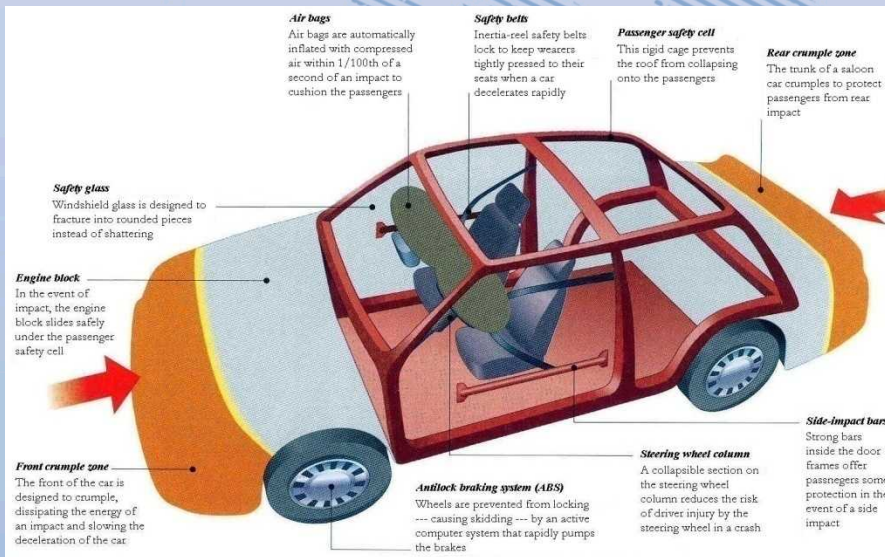
# Routes of Exposure



The PPE used should protect the user from the relevant routes of exposure. This will depend on the organism being used, what quantities, the type of equipment, and what other controls are already in place.

# Risk Mitigation

## Comparison of Car Safety and Motorcycle Safety



Car safety is all about engineering systems

Motorcycle safety is all about PPE

# Risk Mitigation

---

Any questions with regards to **Risk Mitigation** and the **Hierarchy of Controls**?



# Performance

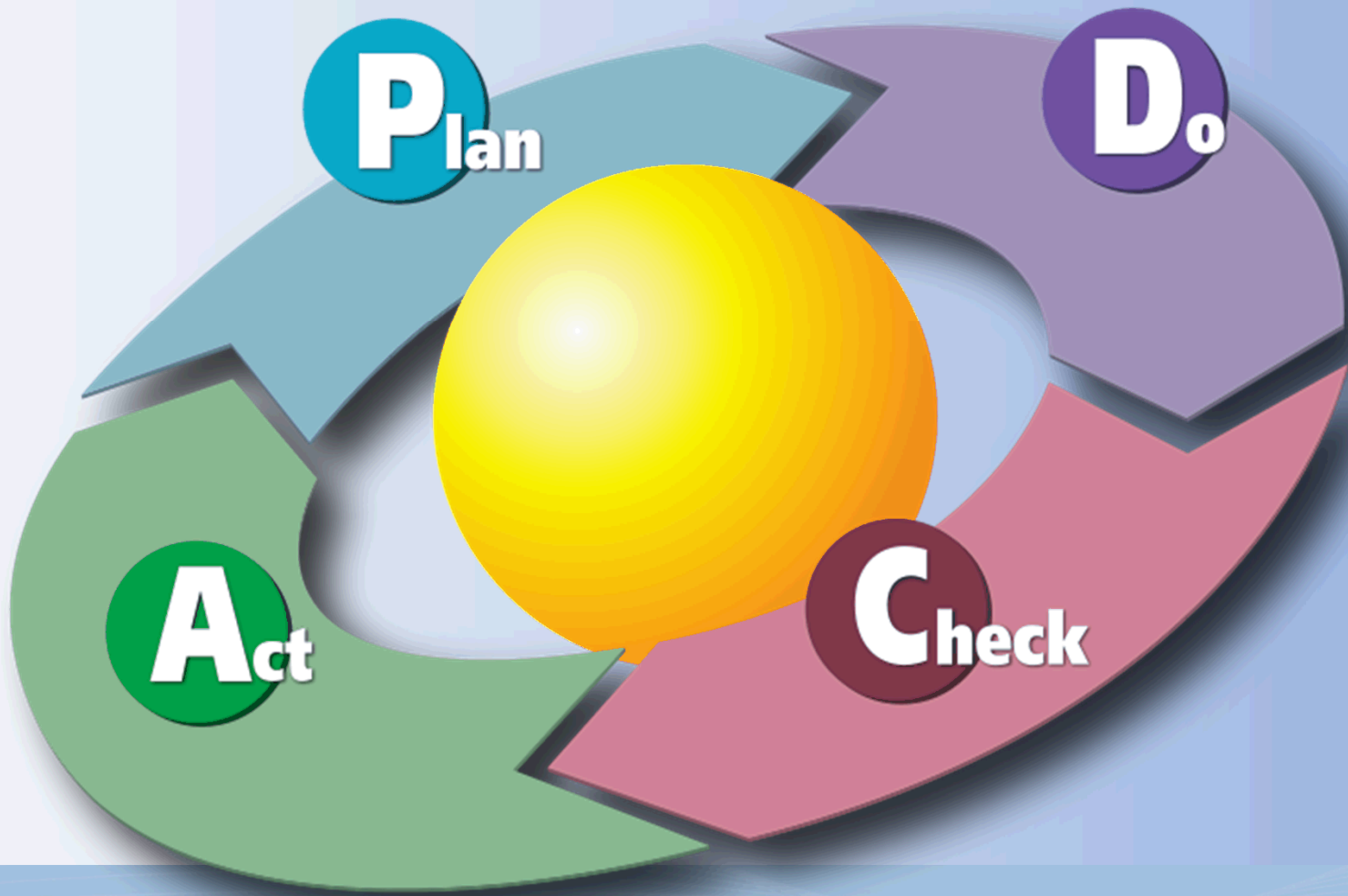
**Question:** After a thorough risk assessment and implementation of appropriate risk mitigation efforts, what is still missing?

## Performance

- The implementation of the entire biorisk management system, including evaluating and ensuring that the system is working the way it was designed. Another aspect of performance is the process of continually improving the system.

# Performance Indicators

- The only way to document effective performance is to measure it
- A measurement is not necessarily a number
- Performance can be measured by looking at both activities and outcomes of a biorisk management system
- Establishing performance indicators must occur during planning objectives, roles, and responsibilities
- Performance indicator measurement collection should be integrated into routine activities.



# Intro to Biosecurity

 Sandia National Laboratories

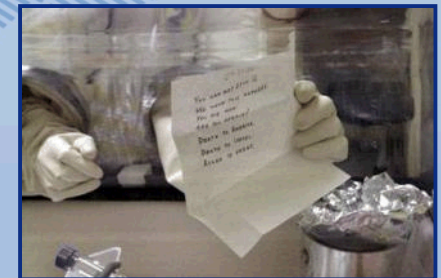
 **International**  
BIOLOGICAL THREAT REDUCTION



# Biosecurity Threats

## Examples

- **Attacks on bioscience facilities** by outside adversaries with the intent to cause harm
  - Stealing: Pathogen collections, Select agents, research animals
  - Arson and sabotage
- **People outside bioscience facilities** who want to obtain pathogens with the intent to commit malicious acts
  - Extremists purchasing pathogens: *Salmonella typhi*, Anthrax, *Clostridium botulinum*, *Yersinia pestis*
- **People within bioscience facilities** using their position to commit malicious acts
  - Stealing pathogens: Anthrax, *Shigella dysenteriae*, *Salmonella typhi*, toxins
  - Research theft: intellectual property – data, materials, cultures



# Unique Challenges

**Discussion:** What are some **unique challenges to securing biological materials in a laboratory**, as opposed to securing:

- Money
- Dangerous Chemicals
- Nuclear Material
- Electronic Information?

*What makes biological materials different?*

# Unique Challenges

- Viruses and Bacteria can **multiply**, making them difficult to count (and thus, keep track of) in the laboratory.
- Potentially, one need only steal a **small amount**... more can always be grown from that seed stock.
- Detection of theft is almost impossible. Vials are small. Biological agents do not give off energy (unlike radiological materials), making stand-off **detection difficult**.



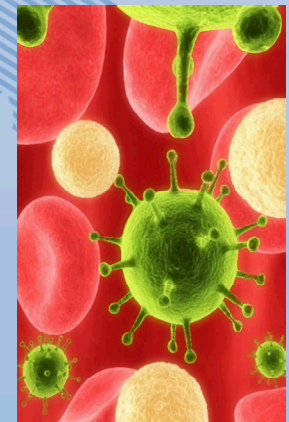
# Unique Challenges

**Question:** Where can you find biological materials in the laboratory?

## What should we protect?

- 1) Only vials with well-characterized strains? Closely related strains? Aliquots?
- 2) Genetic materials? Reagents? Vectors?
- 3) Waste?
- 4) Experimental Results? Sequence Information?
- 5) Animals?

## How should we protect?



# Unique Challenges

**Laboratories**, unlike banks or nuclear repositories, **do not often think of themselves as needing to be secure** – this often requires a **cultural change** toward security.

- 1) For most **laboratory workers**, the idea that their biological materials could be desired for intentional misuse is foreign.
- 2) In **academic** settings, openness is valued.
- 3) In a **clinical** setting, security does not typically consider biological materials.

A proper **Risk Assessment** can help determine security needs

# Unique Challenges Summary

Securing biological materials in the laboratory can be challenging because they can **replicate**, are **hard to detect**, are **found everywhere** and the idea of security in the laboratory setting often requires a **cultural change** as well as good **communication about potential risks**.



# Biosecurity Risk Mitigation

**Biosecurity Risk Mitigation** is the process whereby **risks** identified and characterized during a risk assessment **are reduced through active intervention**, be it **physical** or **procedural**.

**Biosecurity Risk Mitigation** should be based on a **Risk Assessment** including analyzing hypothetical scenarios with a defined **agent, adversary**, and a particular **way** that adversary will attempt to **steal and/or misuse** the biological material.

# Biosecurity Risk Mitigation

**There are five pillars of Biosecurity Risk Mitigation**

- 1) Physical Security**
- 2) Personnel Management
- 3) Material Control & Accountability
- 4) Transport Security
- 5) Information Security

# Physical Security

The first “pillar” is **Physical Security**

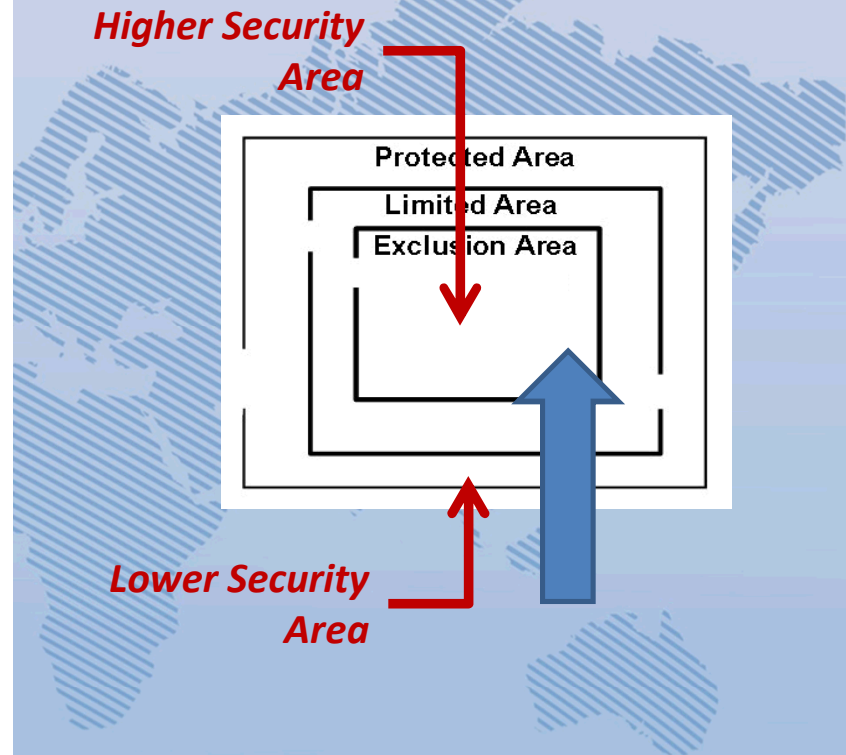
**Physical Security** is the assurance of safety from physical intrusion



# Physical Security

An important concept in **Physical Security** is the concept of **Graded Protection**. This is based on the idea that different areas of a facility will have different **levels of security** based on risk.

**Graded Protection** is manifested in concentric rings of increasing security spanning **from outside to inside** the facility.



# Physical Security

## Graded Protection

### Property Protection Areas (Low risk assets)

- Grounds
- Public access offices
- Warehouses

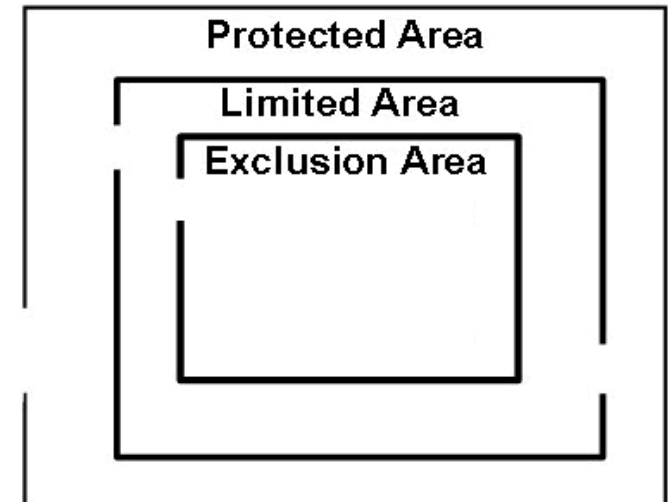
### Limited Areas (Moderate risk assets)

- Laboratories
- Sensitive or administration offices
- Hallways surrounding Exclusion Areas

### Exclusion Areas (High risk assets)

- High containment laboratories
- Computer network hubs

## Concentric Layers of Security



## Question:

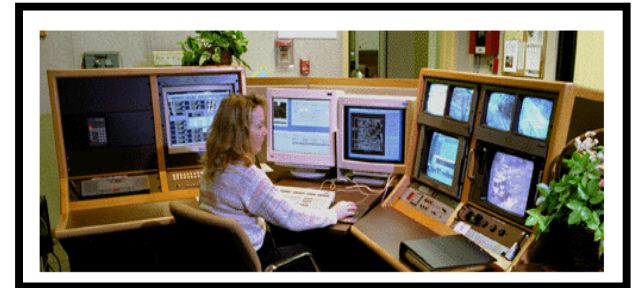
Why is concentric good?

# Physical Security

## 3 Principles of Physical Security:

- **Detection**
- **Delay**
- **Response**

We will also cover **Access Control**, which is another important, overall, aspect of physical security.

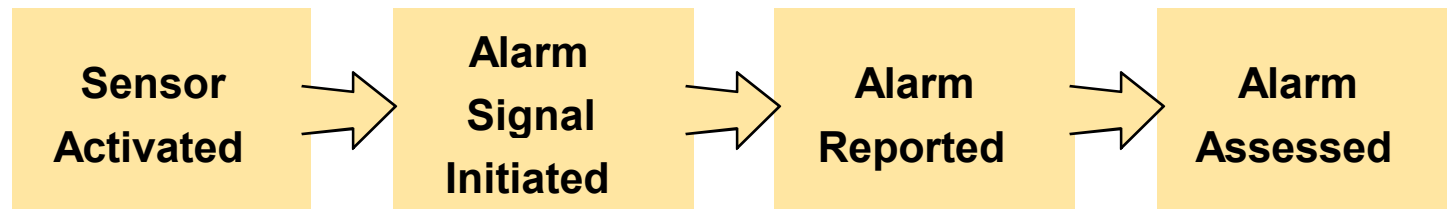


# Physical Security

## Principle 1) **Detection**

Intrusion **Detection** is the process of determining whether an unauthorized action has occurred or is occurring

**Detection** includes sensing the action, communicating the alarm, and assessing the alarm



# Physical Security

Principle 1) **Detection**

**For Example:**



Intrusion **Detection** can be as complicated as a **closed-circuit television system**, infrared and **motion sensors**, and **guards** patrolling throughout the facility.

Or, it could be as simple as good **training** of laboratory staff and a procedure to call someone in case a suspicious person is noticed in the laboratory.

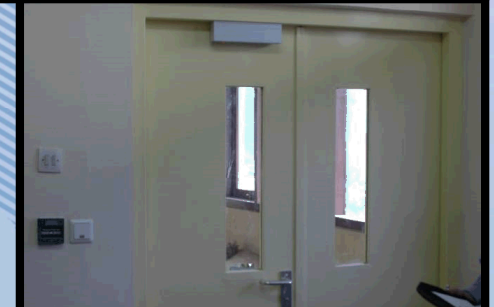
# Physical Security

## Principle 2) **Delay**

**Delay** is simply the act of slowing down an intruder's progress in your facility long enough so that the adversary may be detected, assessed and responded to.

There are many ways of delaying an intruder

- **Perimeter Fencing**
- **Solid doors with locks**
- **Bars on windows**
- **Magnetic switches on doors**



# Physical Security

## Principle 3) **Response**

**Response** is the act of alerting, transporting, and staging a security force to interrupt and neutralize an adversary.

### **Response is tied to the overall system objective**

**Deny:** To prevent an adversary from reaching the target/objective

**Contain:** To 'catch' an adversary before they leave with the target or before they accomplish the objective

# Physical Security

## Principle 3) **Response**

### For Example:

Based on your **Risk Assessment** and **scenario analysis**, **Response** can range from implementing a **guard force** in your facility to establishing a line of **communication** with your local **police force**.

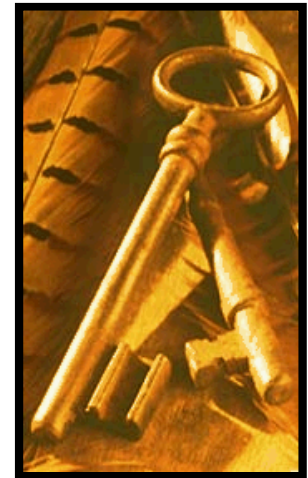


# Physical Security

## Access Control

**Access Control** is another important aspect of biosecurity. It is the mechanism to determine and control authorized entry into secured areas. **Access Control** also provides capability to delay or deny unauthorized personnel.

**Question:** Is there a scenario in which someone would want to allow a person to bypass access controls?



# Physical Security

## Access Control

**For Example**, access granted based on:

### Something you have

Key

Card (Credential)

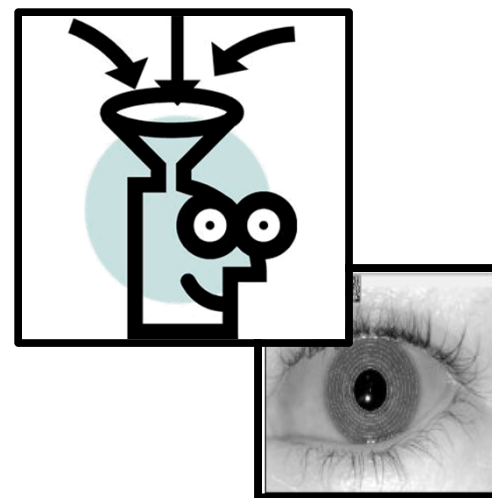
### Something you know

Personal Identification Number (PIN)

Password

### Something you are

Biometric feature (i.e., fingerprints)



# Physical Security

## Discussion:



What do you do in your laboratories at home to prevent people from entering areas they are not supposed to?

# Physical Security Summary

**Physical Security** is the most “traditional” pillar of biosecurity. When people hear “security”, they often think of guards, gates, and guns.

For many **laboratories**, however, physical security may not be the most important aspect of biosecurity. Not too many people from the outside may want to get in, even if there are “desirable” microorganisms. **As an outsider, if you don’t know anything about a laboratory, it may be difficult to find what you are looking for even if physical security is not very good.**

Of course, every system must be designed not on intuition, but after a **robust risk assessment**.

# Biosecurity Risk Mitigation

## There are five pillars of Biosecurity Risk Mitigation

- 1) Physical Security
- 2) Personnel Management**
- 3) Material Control & Accountability
- 4) Transport Security
- 5) Information Security

# Personnel Management

The second “pillar” is **Personnel Management**

**Personnel Management** in the context of biosecurity, it is the assurance that the people that are given access to sensitive biological materials **should** have that access.



# Personnel Management

## The Objectives of a Personnel Management Program are to:

**Understand that human factors can significantly impact the success of biorisk management.**

- To reduce the risk of theft and fraud
- To reduce the risk of scientific misconduct
- Etc..

**To support the procedural and administrative access control requirements**



# Personnel Management

**For Example:** These are some factors that can influence **Human Performance**

- **Job**
  - Setting
  - Values
- **Individual**
  - Personalities
  - Values
- **Organization**
  - Expectations
  - Assessments



# Personnel Management

## Personnel Training – **Security Awareness**

Promoting **security awareness** in employees is one of the most important ways breaches in security can be recognized.

Lab workers should be **aware** of who should be and should not be in their work areas.

### **For Example:**

A person with the wrong type of badge, or simply someone you don't recognize in your part of the building, should be asked: "who are you?" and, if necessary, reported to building security.

# Biosecurity Risk Mitigation

## There are five pillars of Biosecurity Risk Mitigation

- 1) Physical Security
- 2) Personnel Management
- 3) Material Control & Accountability**
- 4) Transport Security
- 5) Information Security

*What makes  
biological  
materials  
different?*

We will also discuss a sixth topic:

- 6) Security Awareness

# Material Control & Accountability

The third “pillar” is **Material Control & Accountability**

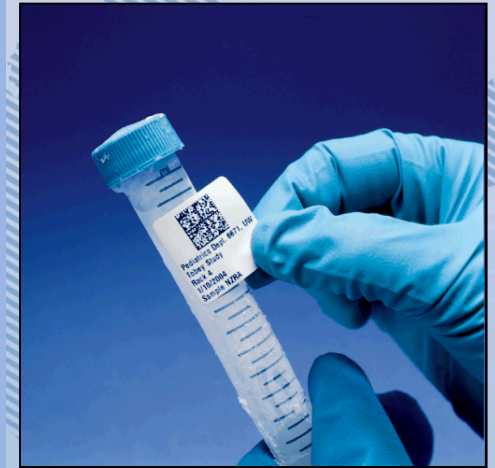
**Material Control & Accountability** is the assurance that there is an awareness of what exists in the laboratory, where it is, and who is responsible for it.



# Material Control & Accountability

The Objective of **MC&A** is to:

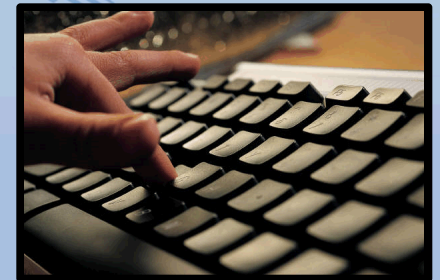
- Ensure the complete and timely knowledge of:
  - What materials exist
  - Where the materials are
  - Who is accountable for them
- Objective is **NOT** to detect whether something is **missing**. This could be impossible. The objective is to create an environment that discourages theft and misuse by establishing oversight.
- Most laboratories already control and track their samples for scientific reasons. The emphasis here is that this is also important from a security perspective.



# Material Control & Accountability

## Key Issues in MC&A

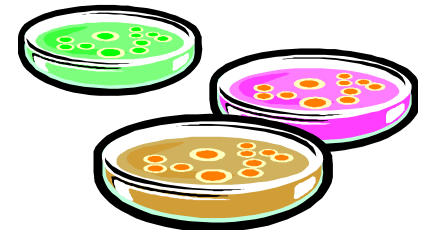
- What materials are subject to MC&A measures?
- What operating procedures are associated with the materials?
  - Where can they be stored and used?
  - How are they identified?
  - How is inventory maintained?
- What records need to be kept for those materials? What timeliness requirements are necessary for those records?
- What does accountability mean?
- What documentation and reporting requirements?



# Material Control & Accountability

## Material Control & Accountability

What information should we keep track of?



Agent	Quantity	Form	Detail	Scope
Which agents?	Any amount of a replicating organism can be significant.	Repository Stocks, Working Samples, yes...	Materials as Items	Laboratory Strains? Wild-type?
Only viable organisms? Whole org. or just DNA?	For toxins, must define a threshold amount.	What about: In host? Contamination?	Each vial as a separate inventory record?	Clinical Samples?

# Material Control & Accountability

## Material Control & Accountability

- **Control is either...**
  - Engineered / Physical
  - Administrative
- **Containment is part of material control**
  - Containment Lab / Freezer / Ampoule
- **Procedures are essential for material control**
  - For both normal and abnormal conditions



# Material Control & Accountability

## Material Control & Accountability

**All material should have an associated “accountable person” who is ultimately responsible for the material.**

- The person best in a position to answer questions about the associated material
- Not someone to blame!
- Ensure that no material is “orphaned”



# Material Control & Accountability

## Discussion:



How is Material Control & Accountability implemented in your laboratory?

# Biosecurity Risk Mitigation

## There are five pillars of Biosecurity Risk Mitigation

- 1) Physical Security
- 2) Personnel Management
- 3) Material Control & Accountability
- 4) Transport Security**
- 5) Information Security

*What makes  
biological  
materials  
different?*

# Transport Security

The fourth “pillar” is **Transport Security**

**Transport Security** is the assurance that the same rigorous processes that protect biological materials in the laboratory follow those materials when they are transported outside laboratory areas.



# Transport Security

## Transport Security

- Aims to reduce the risk of illicit acquisition of *high-risk* biological agents
- Relies on chain of custody principles and end-user agreements

### High risk agents are routinely shipped worldwide for diagnostic and research activities

- A local, national, and international concern
- There is a need to develop a common standard, harmonize regulations for security



# Transport Security

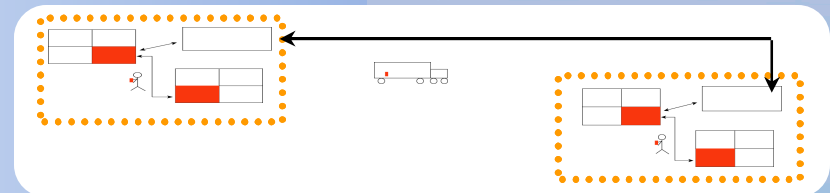
## For example: **Transport**

... is the movement of biological material outside of a restricted area

- Research labs
  - Sample transfers are necessary for study and further research
- Public health labs and diagnostic labs
  - Sample transfers are necessary for diagnosis and analysis

## Transport can occur...

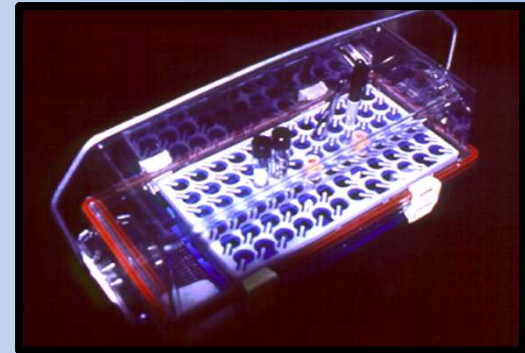
- Across international borders
- Within a country
- Within a facility



# Transport Security

## Internal Transport

- Movement of materials to and from restricted areas **within a facility**
- May involve **Personnel** from
  - Labs
  - Shipping areas
  - Receiving areas
  - Disposal areas (e.g. autoclave and incinerator rooms)
- In order to move materials safely and securely...
  - Pre-approval process
  - Chain of custody



# Transport Security

## External Transport

- Movement of materials **from one facility to another**
- May involve commercial carriers
- Occurs within a wide array of international and state regulations and standards



**Question:** When using a commercial carrier (UPS, FedEx) to ship biological materials, at what point should your responsibility for securing the material end?

# Transport Security

## Chain of Custody (CoC)

### Aims to protect sample by documenting...

- All individuals who have control of sample
- Secure receipt of material at appropriate location

### Chain of custody documentation includes...

- Description of material being moved
- Contact information for a responsible person
- Time/date signatures of every person who assumes control

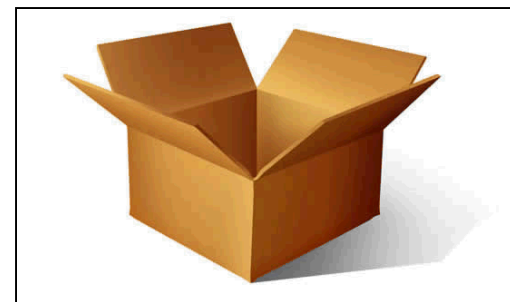


# Transport Security

**So, we want to keep our high-risk samples secure during transport. What should you do?**

- Require a responsible authority to pre-approve all transport
- Advise eligible receiving party of transport
- Document transport in lab records
- Ensure only trustworthy people handle the samples
- Physically secure samples in transit with special packaging and/or locks
- Control movements and document in delivery records
- Use timely shipping methods
- Maintain a Chain of Custody
- Request notification of receipt

**Other ideas?**



# Transport Security

For Example: **When Transporting..**

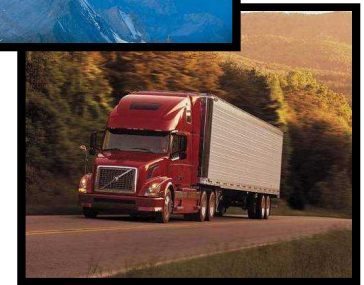
## Moderate risk agents...

- Internal transport personnel screened
- Recipient screened for legitimacy
- Safe receipt notification



## High risk agents...

- Moderate plus
  - Chain of custody
  - Physical controls on storage containers



A proper **Risk Assessment** can help determine transport security needs

# Transport Security

## Discussion:



How are biological materials secured in your laboratory during transport?

# Biosecurity Risk Mitigation

## There are five pillars of Biosecurity Risk Mitigation

- 1) Physical Security
- 2) Personnel Management
- 3) Material Control & Accountability
- 4) Transport Security
- 5) **Information Security**

*What makes  
biological  
materials  
different?*

# Information Security

The fifth “pillar” is **Information Security**

**Information Security** is the assurance that the **sensitive** and **valuable** information stored in a laboratory is protected from theft or diversion.

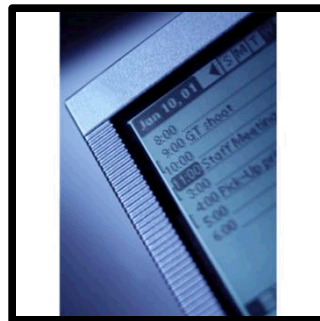
**Question:** What kind of information do you think this might include?  
Work for **5 minutes** with your group and share your ideas with the class.



# Information Security

**Information Security** may not be the most obvious area of biosecurity, but a failure here could have very severe consequences in terms of securing pathogens and toxins.

**Document control** and **computer security** is necessary to reduce risks in a facility. However, these can also be intrusive. Any policies implemented should be based on a **robust risk assessment**.



# Information Security

The Objective of **Information Security** is to:

## **Protect information that is too sensitive for public distribution**

- Label information as restricted
- Limit distribution
- Restrict methods of communication
- Implement network and desktop security

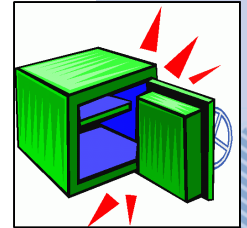
## **Biosecurity-related sensitive information**

- Security of dangerous pathogens and toxins
  - Risk assessments
  - Security system design
- Access authorizations



# Information Security

## Identification, Control, and Marking



### Identification

- Designated sensitivity level
- A review and approval process aids in the identification of sensitivities
  - Critical prior to public release of information

### Control

- Individual responsible for control of sensitive information
  - Physical security
  - Communication security
- In the US, in order to refuse public access upon request, information must be exempt from the Freedom of Information Act

### Marking

- Sensitivity level designation
  - Top and bottom of each page / cover sheet
- Marking and control methods should be well understood by those working with information

# Information Security

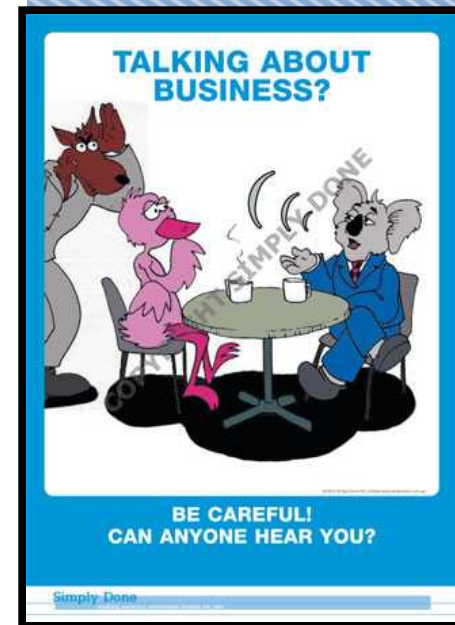
## Communication and Network Security

### Communication Security

- Mail, email, or fax security is required
- Limited discussions in open areas
- Information should only be reproduced when needed and each copy must be controlled as the original

### Network Security

- Firewalls
- User authentication
- Virus protection
- Layered network access
- Desktop security
- Remote and wireless access controls
  - Encryption
  - Authentication



# Information Security

## Security Considerations for Network Systems

### Administrators have full control

- The ultimate insider

### Protect the system using procedures

- Two person control
- Configuration management
- Password control

### Restrict operator privileges

### Provide physical protection for equipment

### Backup equipment and procedures must be provided to maintain security

### Emergency power and uninterruptible power supply required for computers



# End of the Module

Thank You!