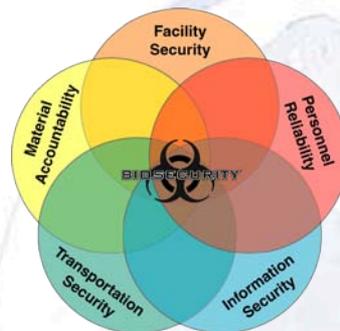




# *Biosecurity Principles*



SAND No. 2005-3288 C

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



# A Focus on the Laboratory

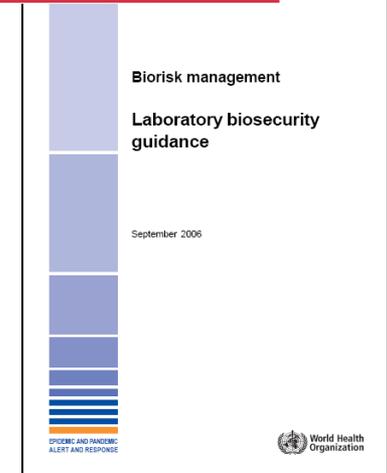
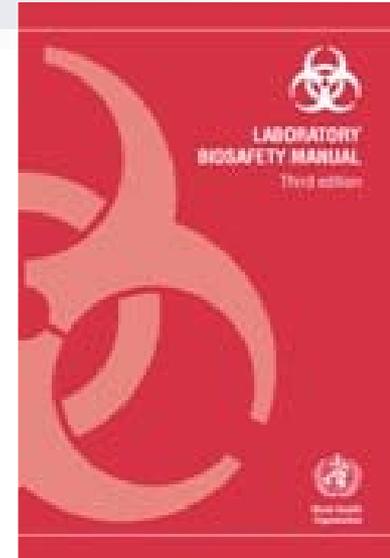
- **Laboratory Biosafety**

A set of preventive measures designed to reduce the risk of accidental exposure to or release of a biological agent

- **Laboratory Biosecurity**

A set of preventive measures designed to reduce the risk of intentional removal (theft) and misuse of a biological agent – intent to cause harm

- **Fundamentally, there are risks to working with pathogens and toxins**





# 1. Biosecurity Discussion

- **What are the primary reasons/drivers for implementing biosecurity?**
- **Are there reasons besides government regulation?**
- **Whose role is it to determine if security is needed?**
- **Whose role is it to determine what type and how much security is needed?**



**“...given the high level of know-how needed to use disease as a weapon to cause mass casualties, the United States should be less concerned that terrorists will become biologists and far more concerned that biologists will become terrorists.”**

**-World At Risk,**

The report of the commission  
on the prevention of  
weapons of mass destruction  
proliferation and terrorism,  
December 2008

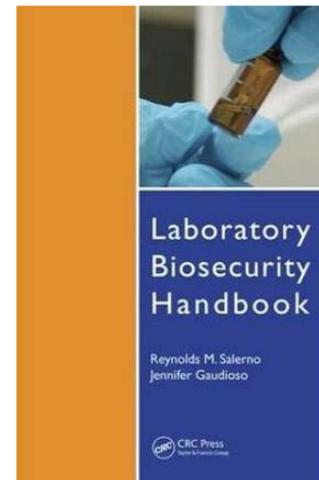
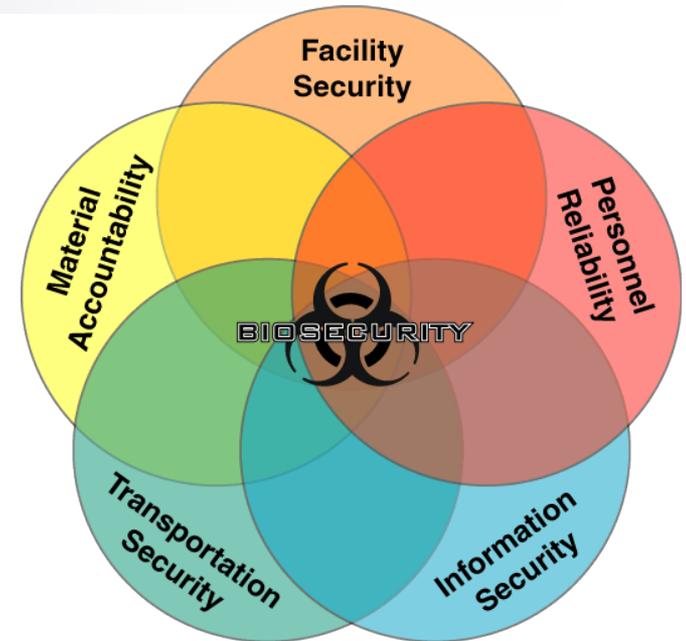


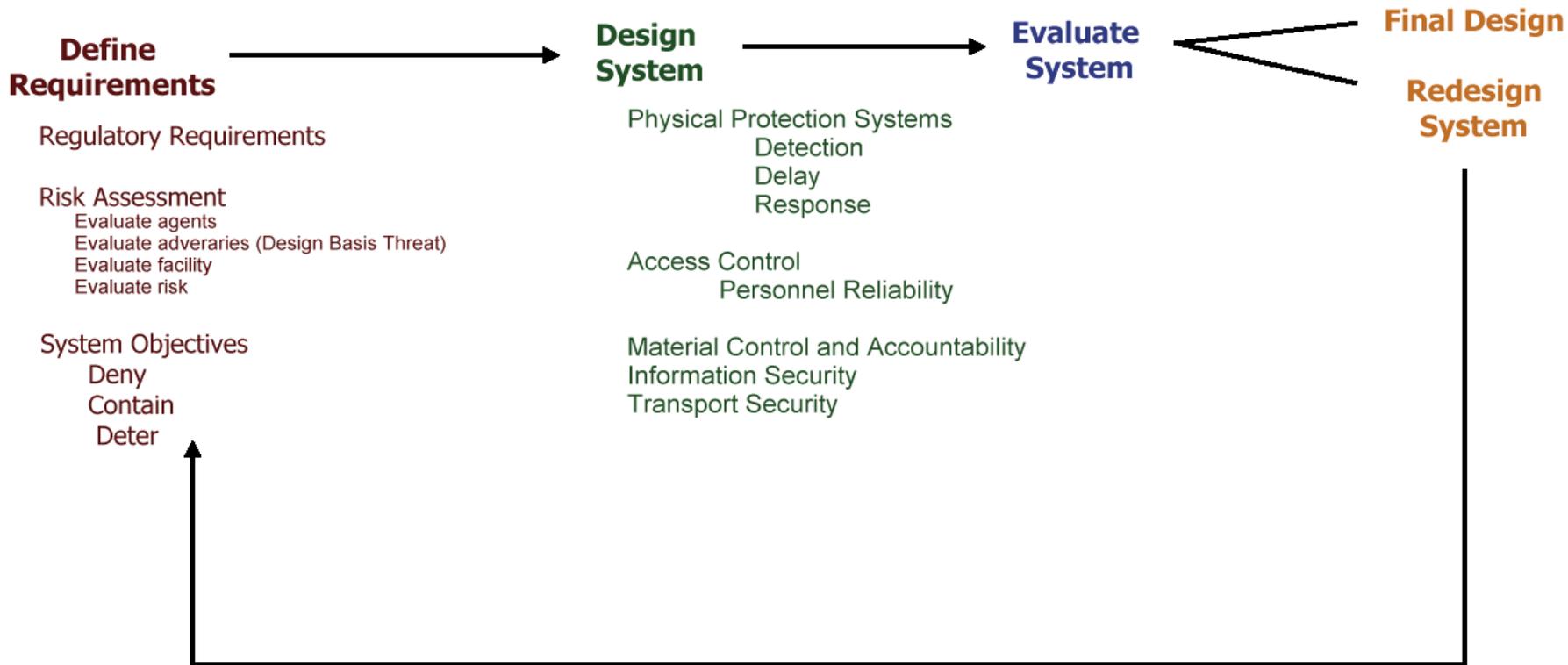
# Biosecurity Systems – A Comprehensive Approach

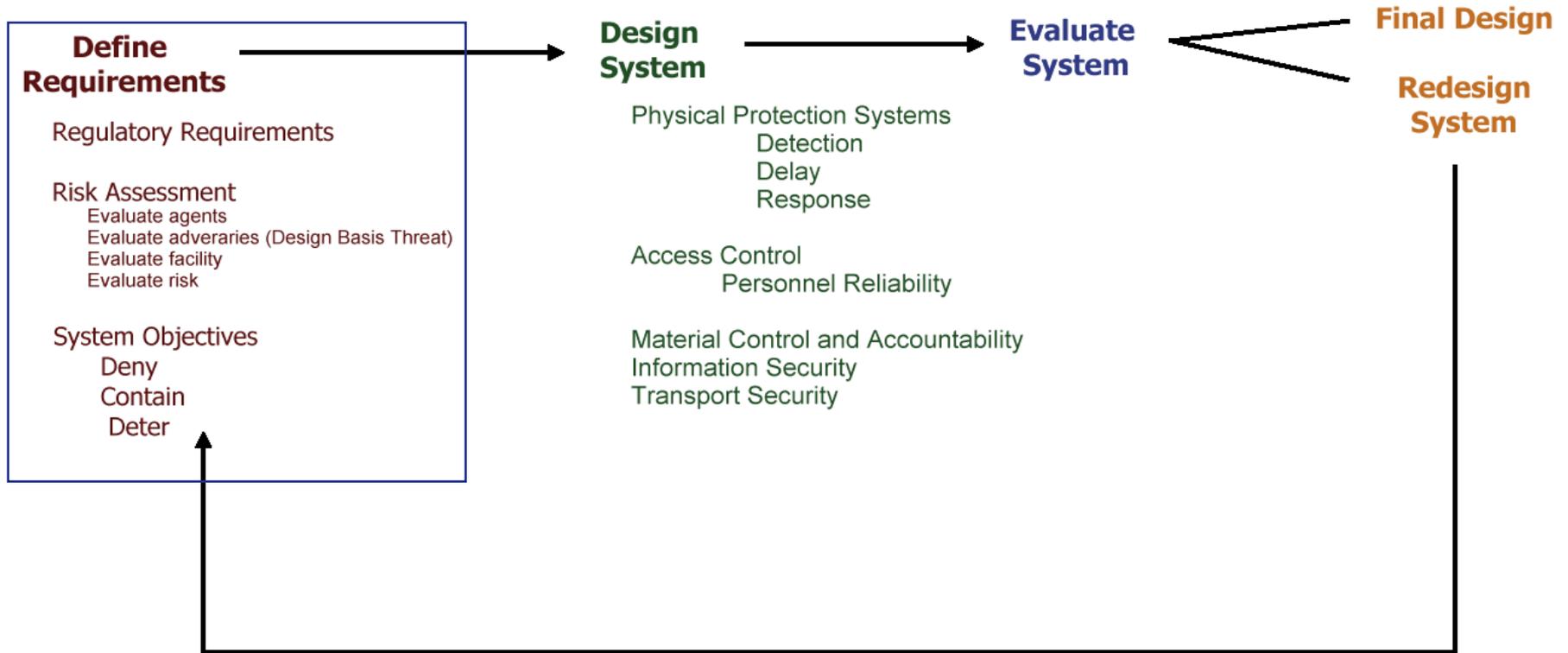
- **Biosecurity system components**

- Physical security
- Personnel security
- Material handling and control measures
- Transport security
- Information security
- Program management practices

- **Each component implemented based on results of risk assessment**









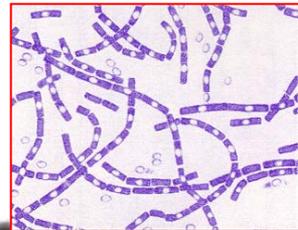
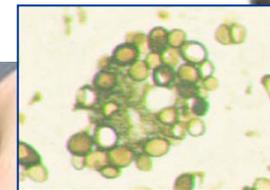
# Define Requirements

- **Management responsible for meeting all international, national, and local regulatory requirements**
  - Biological Weapons Convention**
  - UN Security Council Resolution 1540**
  - National regulations**
  
- **Risk assessment**
  - Gives management a framework to decide which scenarios to are acceptable and which are unacceptable
  - Set performance requirements for the security system



# Risk

- **Is a function of the likelihood an adverse event will occur and its consequences**
- **Work with pathogens will always involve some level of security risk**
  - Distinguish between “acceptable” and “unacceptable” risks
  - Cannot protect against every conceivable adverse event
- **Resources for risk mitigation are not infinite**
  - Existing resources should be used efficiently





# Risk Assessment Process

- **A standardized biological risk assessment process allows the risk assessments to be:**

Repeatable  
Quantifiable

- **A systematic, standardized approach should include:**

Accepted criteria for assessing the risk

A “scoring system” for evaluating the situation against the criteria

A process that ranks the criteria

A process that allows analysis of the risk to identify driving factors and allow better realization of mitigation measures

Enable better communication of risk

- Help to define what is acceptable risk

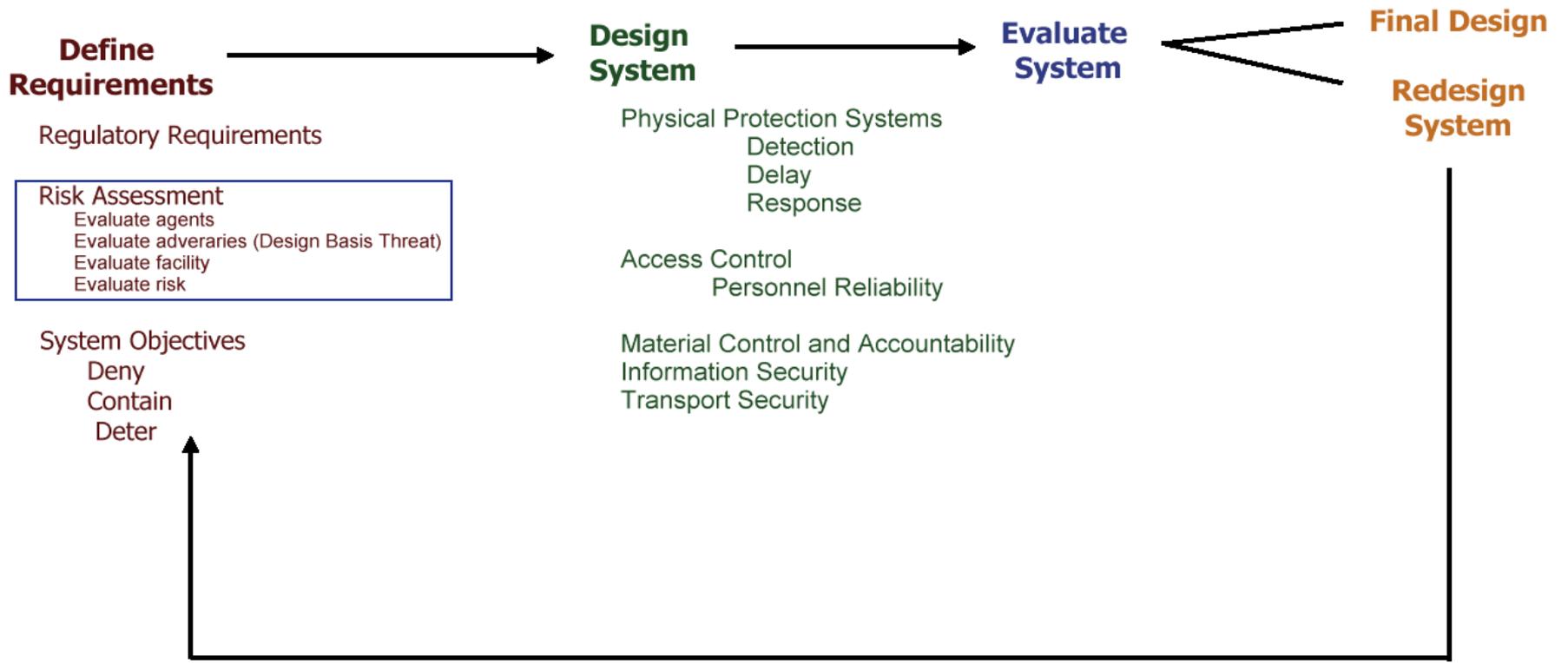




# Laboratory Biosecurity Risks

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

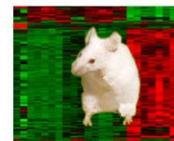
- **Likelihood**  
Of an adversary targeting and successful stealing of a specific biological agent from the laboratory
- **Consequences**  
Of disease from malicious release of the specific biological agent
- **Risks**  
Risk of deliberate exposure to the human community  
Risk of deliberate exposure to the animal community
- **This method can be used to assess and help protect against other security risks (E.g. theft of equipment or sabotage)**





# Biological Agent Risks

- **Not all biological agents have the same risk**
- **Identification of a 'target' is difficult for biological agents/materials**
  - Microbes cannot be counted
  - The 'target' or asset may be all over a room, inside an animal, in the waste system, etc
  - Microbes cannot necessarily be detected if missing (an entire tube may be detected but not a microbe from within)





# Potential Adversaries

## Scenarios involving Insiders generally pose a higher risk than scenarios involving Outsiders

### Insiders

Access to facility and buildings where biological agents are stored and used  
Can wait for an opportune time  
Have knowledge of facility operations and security system  
Some have relevant technical skills and know how to covertly remove the desired biological agent

- **Opportunity – yes**
- **Means – yes**
- **Motive – ?**

### Outsiders

Most biological agents can be readily found elsewhere

- **Other laboratories and in nature**

Do not have authorized access  
Have limited knowledge about facility operations and security  
Will not know exactly where the desired biological agent is stored  
Collusion with an Insider increases risk of detection

- **Opportunity – significantly less**
- **Means – typically less**
- **Motive – ?**



# Design Basis Threat

- **Threat assessment is challenging**

Little information about targeting of bioscience facilities

Little historical data

- **Threats become a policy decision**

Design basis threat is a policy statement that articulates the threats and the security system objectives

- **Design Basis Threat statement**

Should be developed by all stakeholders

- **Scientific and operational personnel at institution**
- **Signed by Head of institution or other responsible decision maker**





# Illustrative Case: Ft. Detrick attempt, 1970

- **Location:**

Fort Detrick, Maryland

- **Perpetrator:**

Weathermen / Weather Underground

- **Means:**

Attempted to blackmail a homosexual army officer at Fort Detrick into providing them with dangerous bacteria

- **Objective:**

The weathermen were looking for a bacteria that would bypass the filtering system of a city and incapacitate the population for 7-10 days



## Toxic Terror

By Jonathan B. Tucker

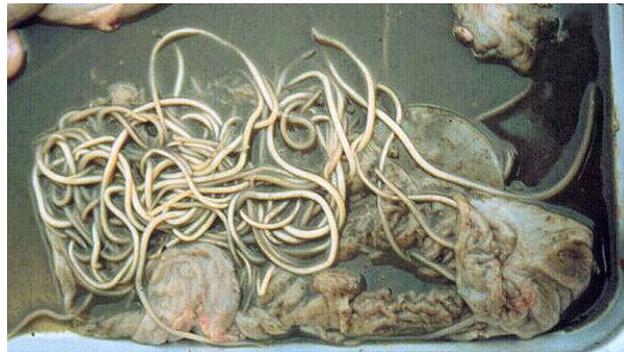
Associated Press, "Plot to steal germs told," reprinted in the Chicago Tribune, November 21, 1970, p.11



# Illustrative Case: Eric Kranz, February 1970



- **Location:**  
MacDonald college in Canada
- **Perpetrator:**  
Eric Kranz, Postgraduate student in Parasitology
- **Means:**  
Theft of *Ascaris Suum* from his college laboratory
- **Objective:**  
Revenge after he was kicked out of his house by his four roommates for not paying his share of the rent
- **Dissemination:**  
Contaminated food in the house with *Ascaris suum* before he left
  - Two of the boys suffered acute respiratory failure
- **Outcome:**  
Kranz was tried for attempted murder





# Assessing Threats

- **Motive**

The reason for the crime. Motivations include ideological, personal, economic, and psychotic. Motivations give rise to a particular intent or objectives. They also impact behavior (e.g., passive or active, violent or nonviolent).

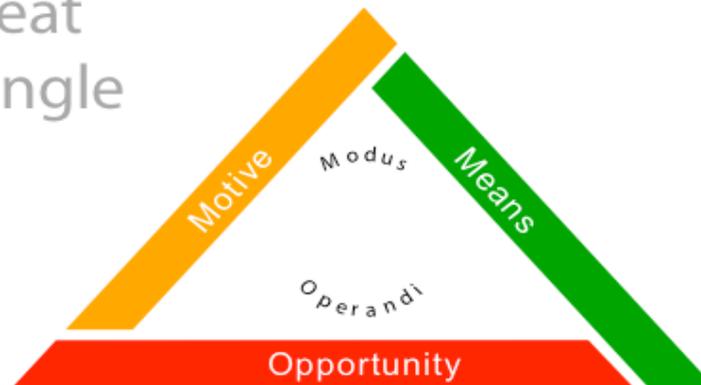
- **Means**

The tools used to commit the crime. Tools include: knowledge (general and specific); equipment (e.g., tools, weapons, explosives, transportation); and people (willing, coerced or unknowing). For an outsider – an insider can be a tool.

- **Opportunity**

The occasion that presents itself to allow a crime (e.g., theft or sabotage) to take place.

The  
Threat  
Triangle



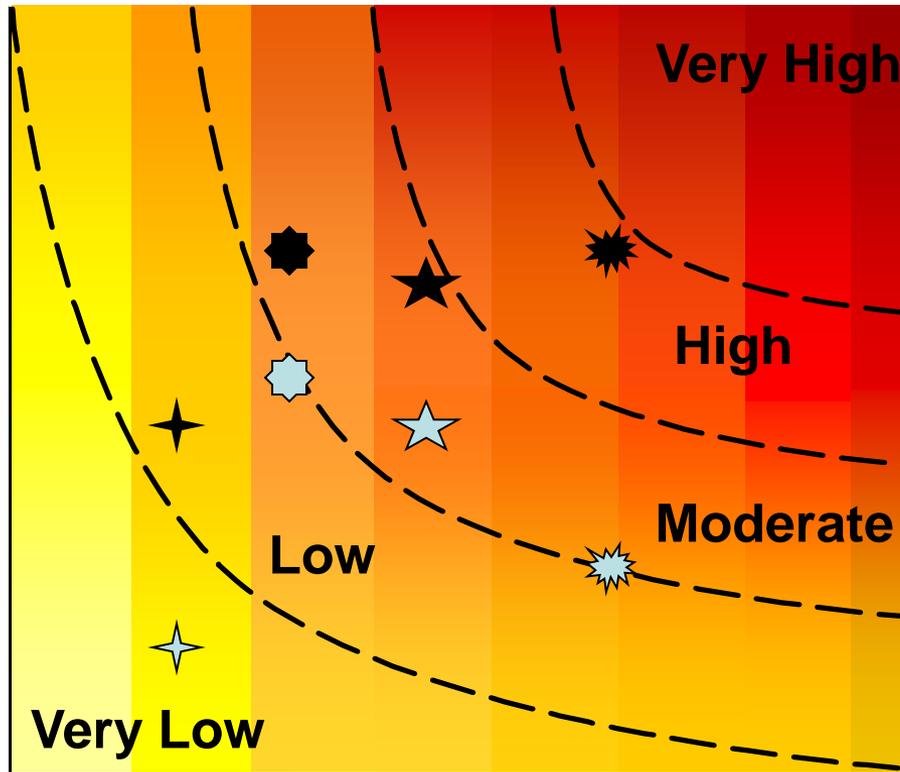


# Assess the Facility

- **Identify mechanisms each defined adversary could achieve their objective**
- **Identify vulnerabilities in the biosecurity system**
  - Physical security
  - Personnel security
  - Material handling and control measures
  - Transport security
  - Information security
  - Program management practices

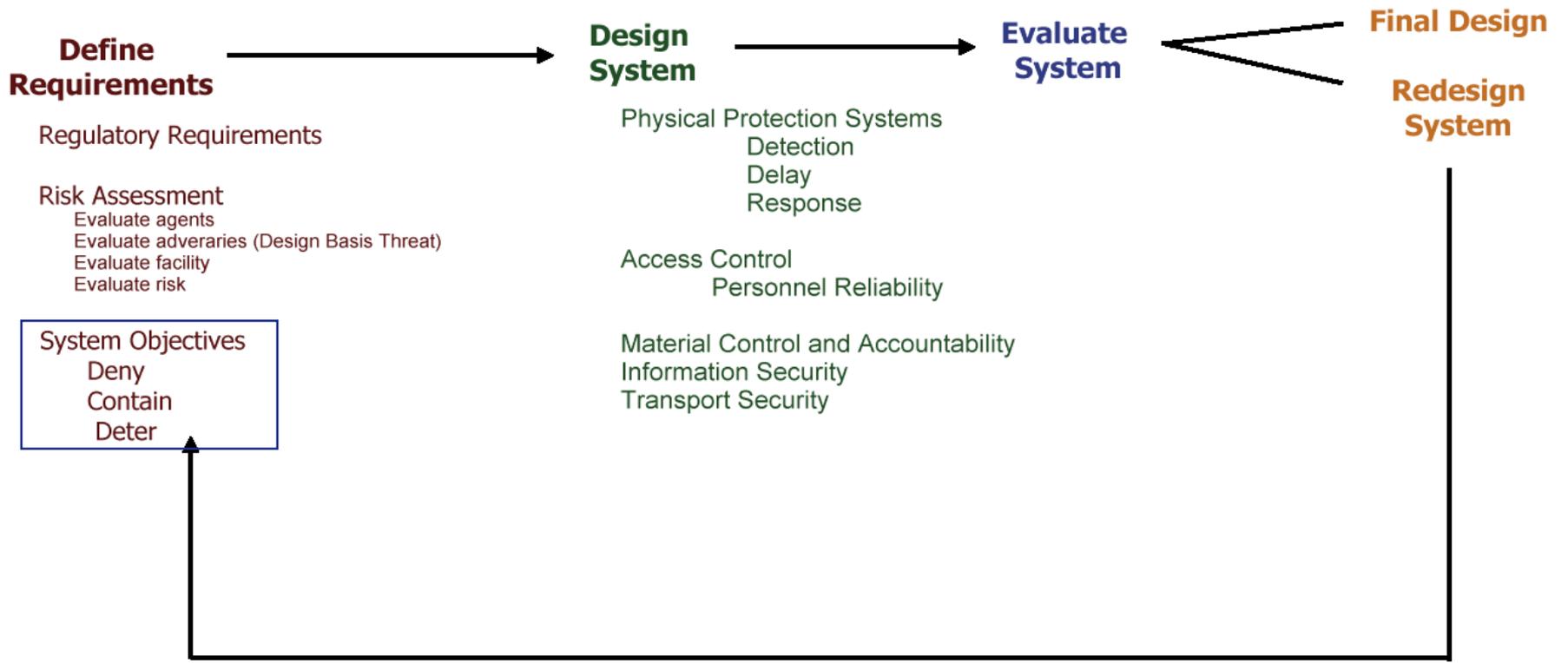


# Characterize the Risk



- Protect against unacceptable risk scenarios

- Develop incident response plans for acceptable risk scenarios





# Define System Objectives

- **Management determines security system strategy:**

Deny: prevent adversary from gaining access to particular pathogen or toxin

Contain: prevent adversary from leaving facility while in possession of stolen pathogen or toxin

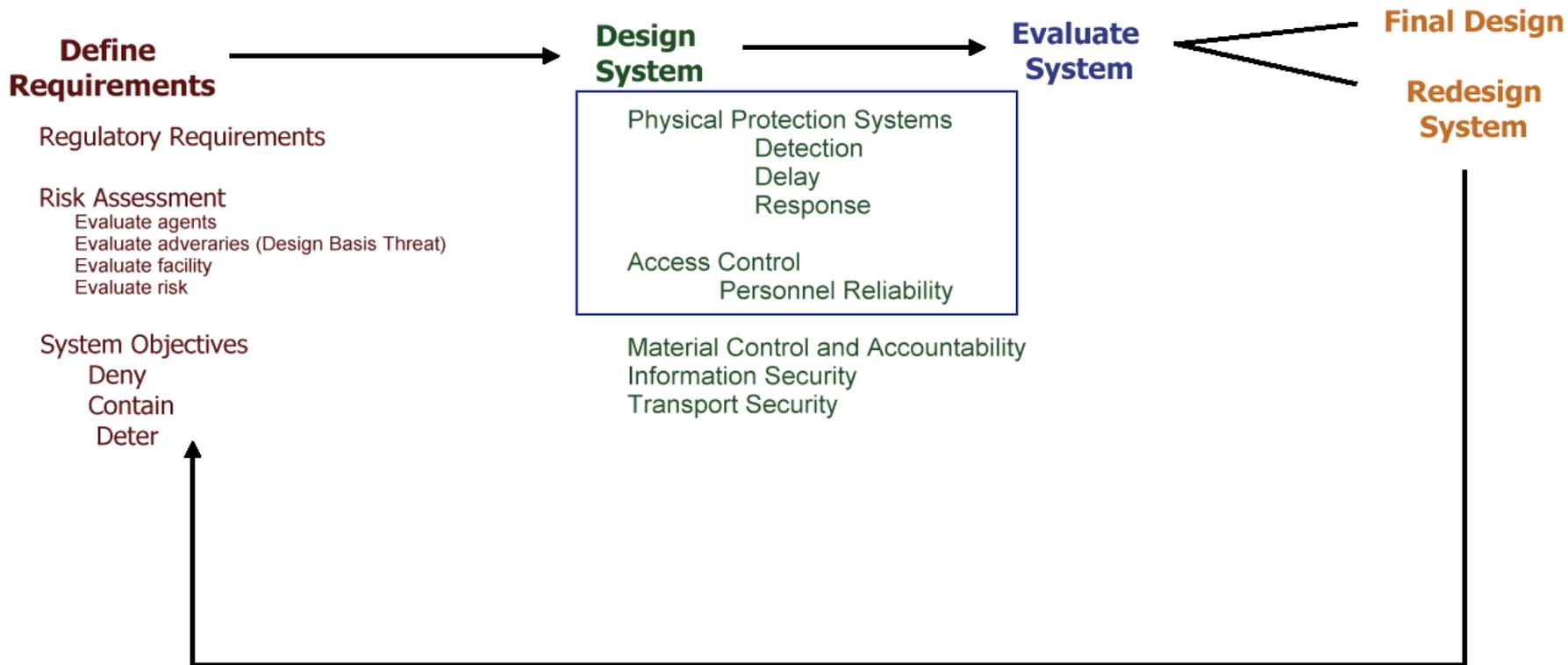
Deter: discourage adversary from stealing a particular pathogen or toxin by making theft of that agent appear very difficult





## 2. System Objective Discussion

- What would the *System Objective* be for a human diagnostic laboratory: to deny, to contain, or to deter, and why?
- What would the *System Objective* be for a typical select agent university research laboratory and why?
- What would the *System Objective* be for a facility containing the smallpox virus and why?





# Physical Protection System Principles

- **Detection**

Intrusion Detection is the process to determine that an unauthorized action has occurred or is occurring

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

- **Delay**

Slowing down an adversary's progress

- **Response**

The act of alerting, transporting, and staging a security force to interrupt and neutralize the adversary

Mitigation and recovery interface with the response function

- **Access Control**

The mechanism to 'by pass' the physical security system



# Graded Protection for Bioscience Laboratories

## Property Protection Areas

- Low risk assets

## Limited Areas

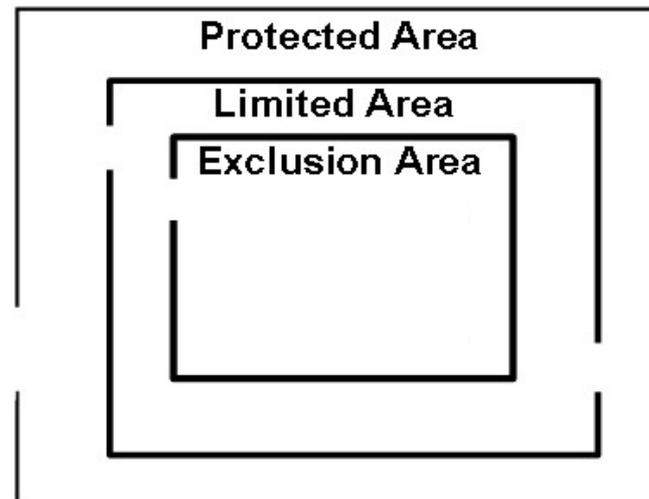
- Moderate risk assets

## Exclusion Areas

- High risk assets

In what security layer (property protection, limited or exclusion area) would you place the following:

- Administration offices
- Clean animals
- Non-infectious bacteria (E-coli K12)
- Multi-drug resistant strain of *M. tuberculosis*
- Frozen vial containing Spanish Flu

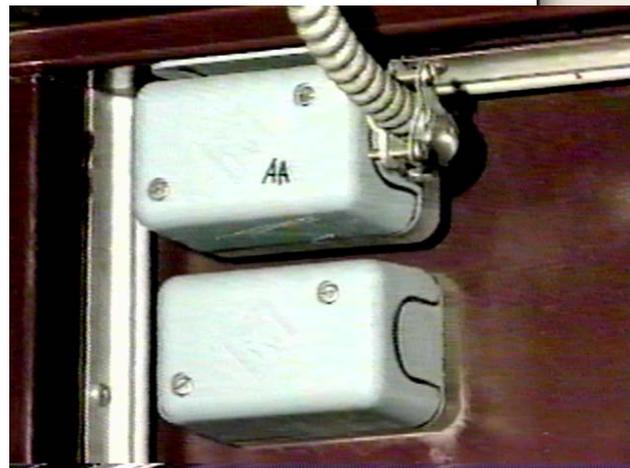




# Intrusion Detection

- **Detect unauthorized access**
- **Many types of intrusion detection**

Personnel notice unauthorized access  
Electronic Sensor





# Video Assessment vs. Video Surveillance

- **Assessment**

Alarm information triggered by sensor activation and directed to a human to determine if unauthorized access has occurred

Cameras can be used to communicate

Humans can directly observe

- **Surveillance**

Continuous use of a human as a intrusion detector to monitor several restricted areas

Systems often have many cameras

Someone must watch all video screens all the time





# Delay

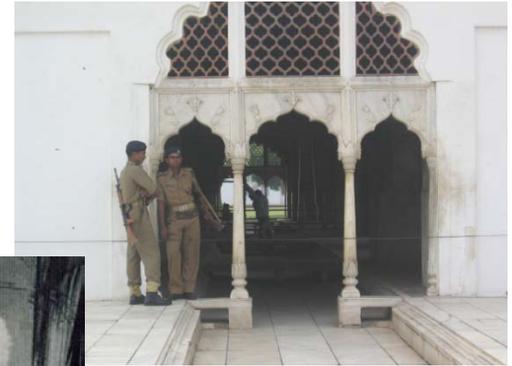
- **Slow down an intruder**
- **Detection should come before delay**
- **Many types of delay methods**
  - Guards
  - Perimeter Fencing
  - Solid doors with locks
  - Bars on windows
  - Magnetic switches on doors





# Guards

- Guards delay and detect the intruders and in some cases also provide response





# Response

- **The objective of 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

Deter: To initiate consequence mitigation measures



# Response Force

- **On-site guard force**

Patrols perimeter and buildings

Summons and directs local law enforcement

Deters

Can be the primary response depending on the motives of the adversary

Information gathering for secondary response

- **Local law enforcement**

Secondary response

Reinforce on-site guard force

- **Respond according to plan when summoned**
- **Equipped and authorized to confront adversary**





# Response Force Requirements

- **Qualification and training**
  - Enforcement responsibilities and skills
  - Equipment familiarity and training
  - Familiarity with facility features and operations
  - Knowledge of restricted area access and biosafety
- **Guard Force Orders**
  - List specific duties and limits of authority
  - Procedures for response to specific alarm conditions
  - Emergency response procedures
  - Notification list
- **Memorandum of understanding with local law enforcement**
  - Specific instructions and agreements
  - On-site training and orientation



# Access Control

---

- **Mechanism to 'by-pass' security system**
- **Allow entry of**  
Authorized persons
- **Prevent entry of**  
Unauthorized persons
- **Allow exit of**  
Authorized persons



# Basis of Access Controls

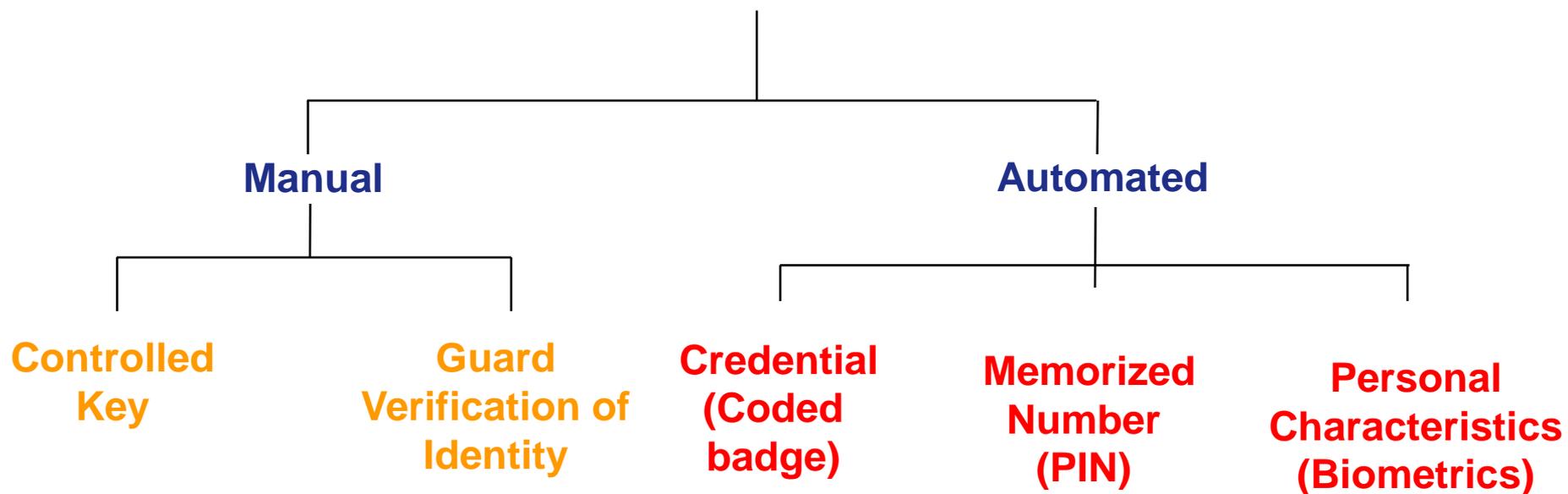
- **Something you have**
  - Key
  - Card
- **Something you know**
  - Personal Identification Number (PIN)
  - Password
- **Something you are**
  - Biometric feature (i.e., fingerprints, face)
- **Combining factors greatly increases security**





# Access Control Techniques

## Personnel Entry Control





# Examples of Electronic Access Controls

- **Coded Badges**

- Proximity Cards
- Magnetic Stripe Badges
- Wiegand Cards
- Smart Cards



- **Biometrics**

- Fingerprint Scanner
- Hand Geometry Scanner
- Iris Scanner





# Key Considerations in Selecting Access Controls

- **Access control systems**

Can be low or high tech

Give varying levels of assurance of person's identity

- **Risk assessment!**

Have error rates and enrollment issues

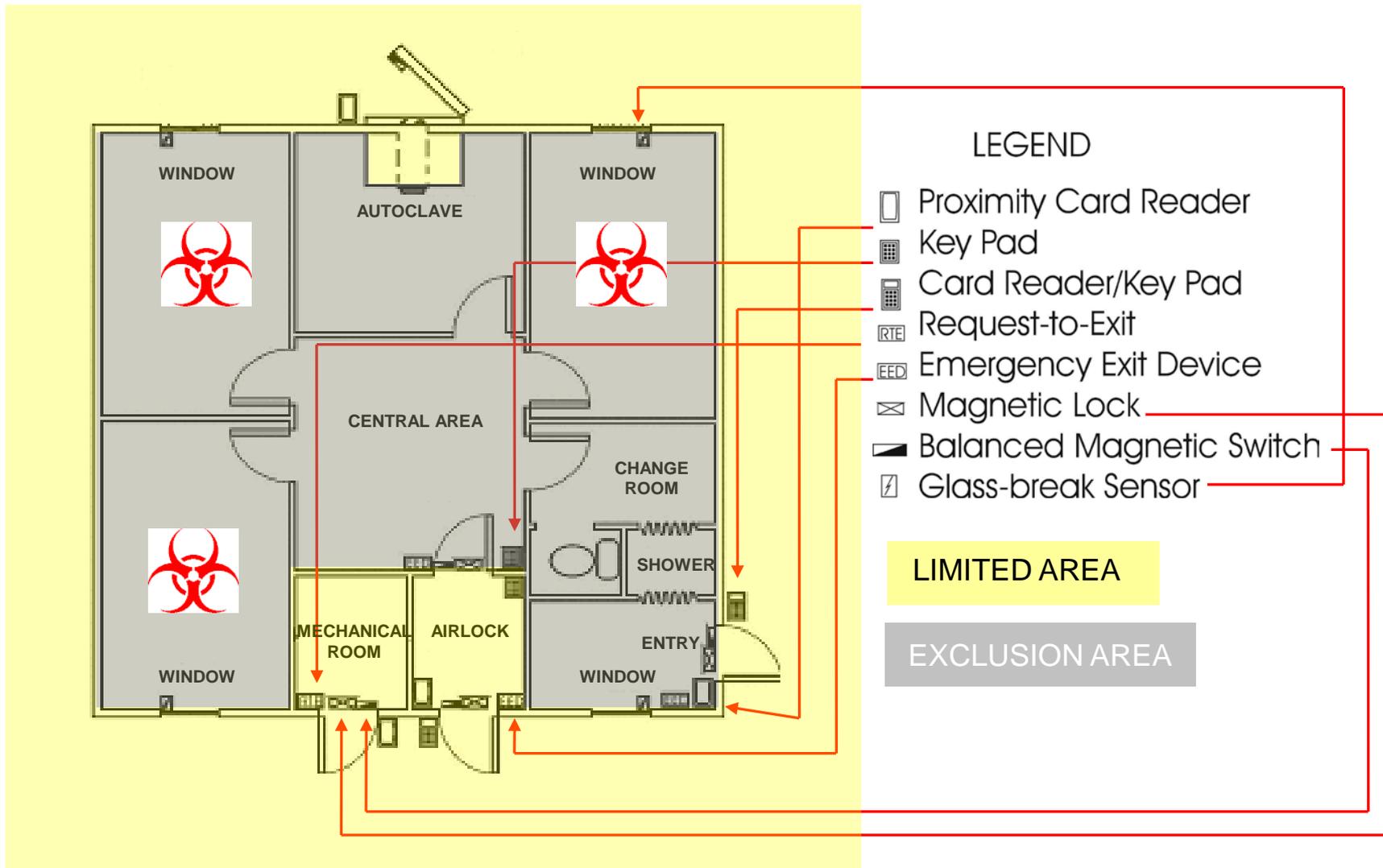
- **1-3% of the population is incompatible with any biometric device**
- **Must have secondary method for those who cannot pass automated inspection**

Needs to accommodate peak loads

Should be designed for both entry and exit



# Physical Security: Example Laboratory Building





### 3. Physical Protection System Discussion

- **What types of detection devices would be appropriate in a bioscience facility and why?**  
Are there types of detection devices that can not be used and why?
- **What are appropriate delay mechanisms for a bioscience facility?**
- **How should a bioscience facility respond to an alarm?**
- **What types of access controls can be used?**  
Where?  
Are there types that can not be used in a bioscience facility and why?



**“Somebody once said that in looking for people to hire, you look for three qualities: integrity, intelligence, and energy. And if they don't have the first, the other two will kill you. You think about it; it's true. If you hire somebody without the first, you really want them to be dumb and lazy.”**

**- Warren Buffett**



# Personnel Reliability

- **The objectives of a personnel reliability program are to**

Help to judge a person's integrity

- **E.g. reduce the risk of theft or fraud**
- **E.g. reduce the risk of scientific misconduct**

To support the procedural and administrative access control requirements

To support the biosafety program





# Which Personnel to Vet?

- **Insiders**

Have authorized access to the facility, dangerous pathogens, and/or restricted information

The insider depends on a facility's access controls and visitor controls

- **Not all positions present the same risk**

Consider the potential consequences

Consider not just the researchers but those also with access like the security force, system/network administrators, locksmith, etc.



# Approaches for Vetting Individuals

- **Public records**

Use governed by Fair Credit Reporting Act  
May also be applicable state and local regulations

- **Interviews**

- **Personality testing**

- **Skill testing**

- **Drug testing**

- **Considerations**

Accuracy of information obtained during vetting process

Have applicant sign “release of information” statement

If periodic reinvestigations will be required, notify applicant during hiring process

Legal constraints on use of information for employment decisions





# National Checks

- **Individual's can obtain a National Police Criminal History Record**
- **Institutions can pay commercial investigators to conduct background screening on potential/current employees**
- **Institutions can run background checks using publically accessible information**
  - Educational Records
  - Profession Credentials
  - Military Records
  - Court Records
  - Criminal Checks
  - Financial Checks





# Reinvestigations

- **A security reinvestigation establishes any security related changes in a person's life**

The same checks are typically run as in initial investigation

Timeline from last investigation to present

Identifies changes like

- **New personal contacts**
- **New financial situations**
- **Situations which should have been reported**
- **Discrepancies from past investigations**





## 4. Background Screening **Discussion**

- **Should individuals working in all areas of a bioscience facility require the same level of screening?**
- **Which individuals are not currently screened?**
- **Is the current background screening process sufficient for those working with biological agents?**
- **Are screening process sufficient for visitors? What about long-term visitors from a foreign country?**



# In-Processing

- **Program should document the steps necessary prior to granting an individual authorized access, e.g.**

Background investigation

Safety and security training

Job –specific briefing

Immunizations

- **Where do new hires work until vetting process and trainings are complete?**

Can take months to years depending on process





# Out-Processing

- **Change access**

Do combination locks need to be changed?



- **Retrieve property, including**

Badges, keys

Laboratory notebooks

Pathogenic materials

Laptops, PDAs, cell phones, pagers

Library materials



- **Deactivate computer and electronic access accounts**

- **If appropriate, notification of Responsible Official to change Select Agent program registration**



# Badges

- **Badges should be issued to those individuals authorized to be in restricted areas**
- **Badge information should include**
  - Individual's name
  - Individual's photograph
  - Expiration date
  - Indication of areas where individual has authorized access
- **Badge return**
  - Upon employee termination
  - Daily or at the conclusion of a limited term for visitors
- **Report lost or stolen badges**





# Visitor Controls

- **Types**

  - Personal Visitors

    - Family members

  - Casual Visitors

    - Tours, seminars
    - Equipment repair technicians

  - Working Visitors

    - Visiting researchers
    - Facility maintenance personnel

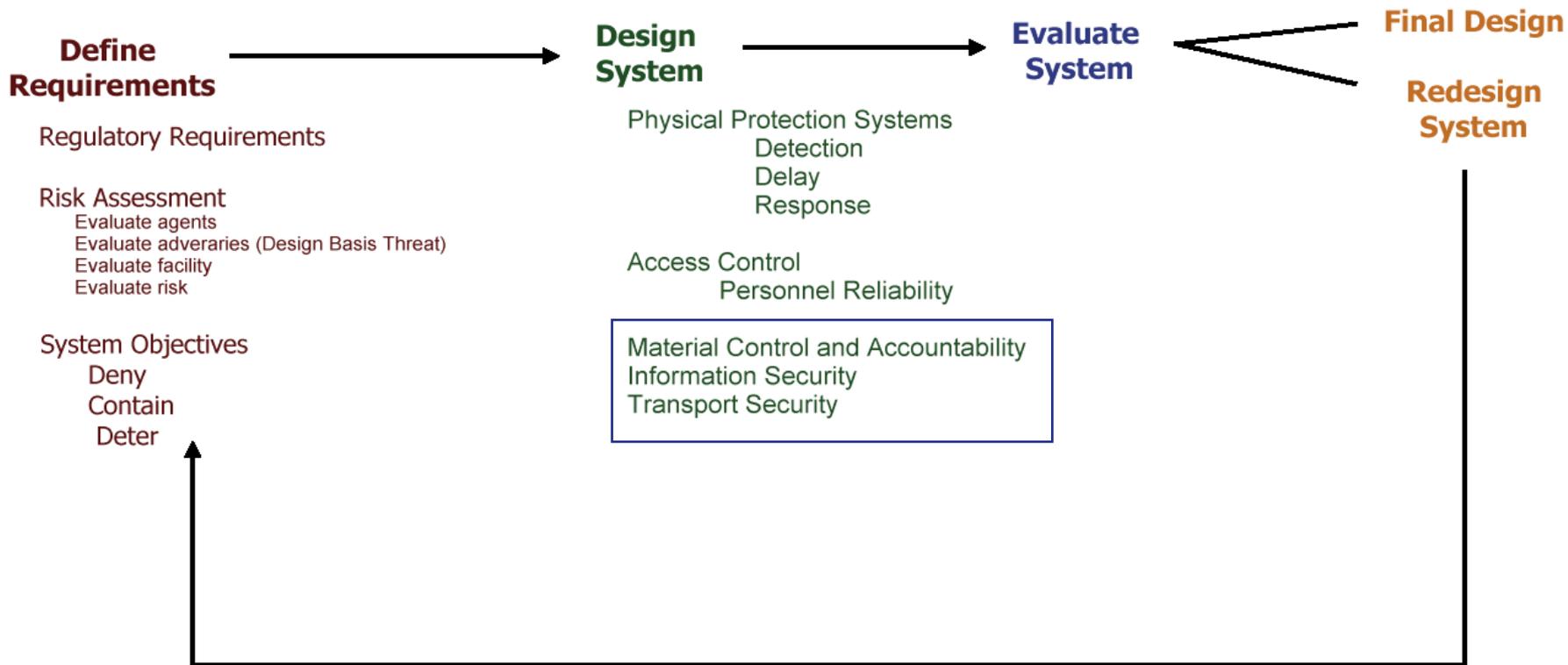
- **Controls**

  - All visitors should have a host at the facility

  - Visitors should be escorted in restricted areas

  - Institution needs to establish policy on amount advance notice required for each type of visitor







# Material Control and Accountability

- **Material Control and Accountability (MC&A) ensure complete and timely knowledge of:**
  - What materials exist**
  - Where the materials are**
  - Who is accountable for them**
- **NOT: to detect whether something is missing**





## 5. Material Control and Accountability Discussion

**Much of MC&A is likely already done for reasons other than biosecurity...**

What are some of the reasons you think a bioscience facility should implement MC&A besides for biosecurity?

What details should be in a laboratory inventory and are they feasible with biological agents?

What is the span of the MC&A program? (E.g. from a blood sample submitted for diagnosis until the sample and all other items used in diagnosis destroyed?)



# Material Control & Accountability Examples

- **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



- **High risk biological agents**

Moderate plus

- **Increased control over working stocks**



# Information Security

- **Protect information that is too sensitive for public distribution**
- **Risks to information include**
  - Loss of integrity
  - Loss of confidentiality
  - Loss of availability
- **Biosecurity-related sensitive information**
  - Security of dangerous pathogens and toxins
    - E.g. Risk assessments
    - E.g. Security system design
  - Access authorizations





# Tamper Indication / Data Authentication

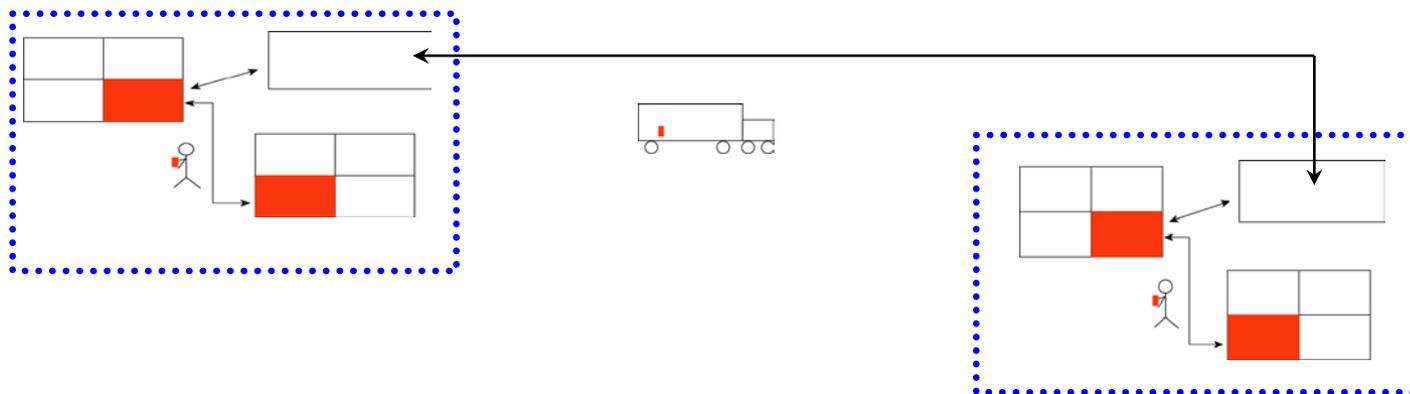
- **Tamper indication and data authentication should be used to monitor the integrity and identity system components**
- **Tamper indication**
  - Verifies the physical integrity
- **Data Authentication**
  - Verifies the originator of data
  - Verifies the data has not been altered between the source and the destination
- **Why authenticate?**
  - Prevent spoofing
  - Prevent substitution
  - Prevent replay old data





# Infectious Substance Transport

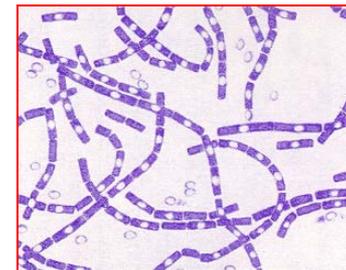
- **Transport – movement of biological material outside of a restricted area**
- **Transport can occur**
  - Across international borders
  - Within a country
  - Within a facility
- **Protection while in transport should be comparable that in the restricted area**
  - May require a documented chain of control



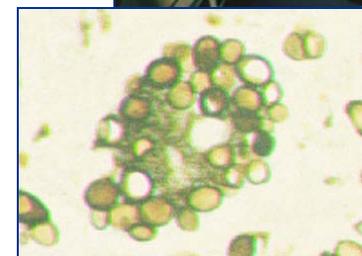
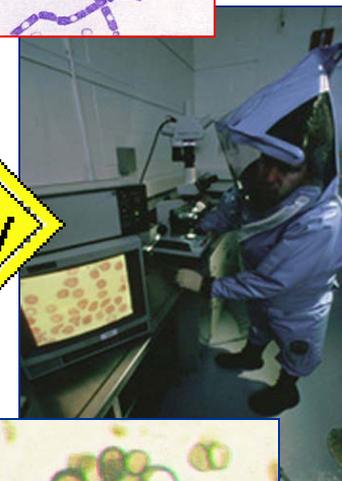


# Hazardous Material Transportation Security

- **Infectious substances (Class 6.2) and toxins (Class 6.1) are defined as Hazardous Material**
- **49 Code of Federal Regulations (CFR) 172 (2003) – HM 232 – mandates security measures for the transport of some Hazardous Material**
  - Select Agents regulated under 42 CFR 73 and 9 CFR 121 require Hazardous Material transport security measures
- **Hazardous Material regulated security requirements include:**
  - Training
    - Security awareness training
    - Specific training as appropriate
  - Written security plan
    - Based on assessment of transportation security risks
    - Address personnel security, unauthorized access, en route security



*Bacillus anthracis*





## 6. Transport Security Discussion

- **What level elements of transport security should be implemented for internal facility transport of the following biological agents?**

Non-infectious bacteria (*E-coli K12*)

Multi-drug resistant strain of *M. tuberculosis*

Frozen vial containing the Spanish Flu (1918 Influenza strain)

- **What measures would you add for external transport for the same biological agents?**



## Define Requirements

Regulatory Requirements

### Risk Assessment

Evaluate agents  
Evaluate adversaries (Design Basis Threat)  
Evaluate facility  
Evaluate risk

### System Objectives

Deny  
Contain  
Deter

## Design System

Physical Protection Systems  
Detection  
Delay  
Response

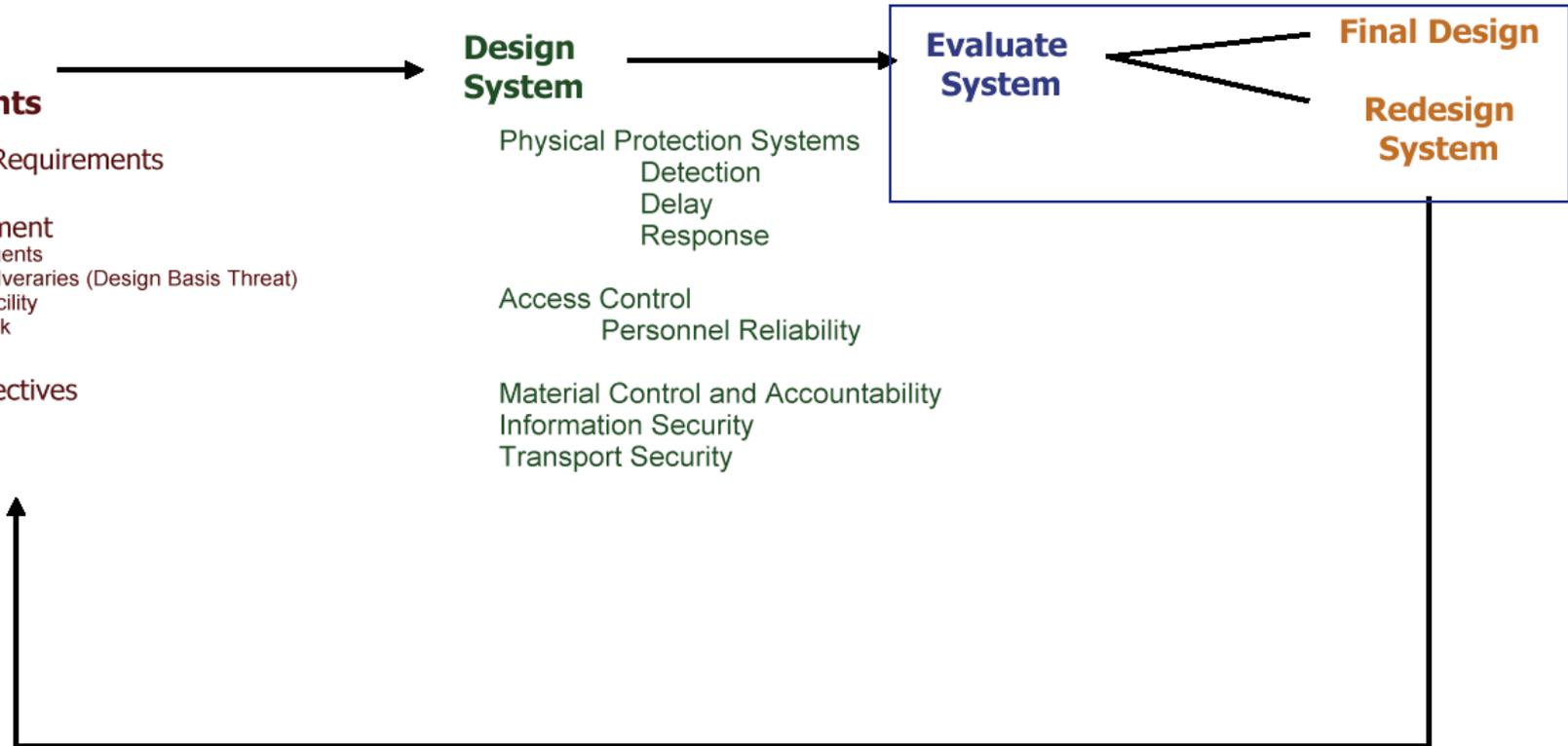
Access Control  
Personnel Reliability

Material Control and Accountability  
Information Security  
Transport Security

## Evaluate System

## Final Design

## Redesign System





## 7. Security Violations Discussion

- What are some examples of security violations?
- How could they be prevented?
- How should management deal with security violations?





# International Calls for Biorisk Management

- **Laboratory Biorisk Management Standard**

Risk-based approach

CWA 15793:2008

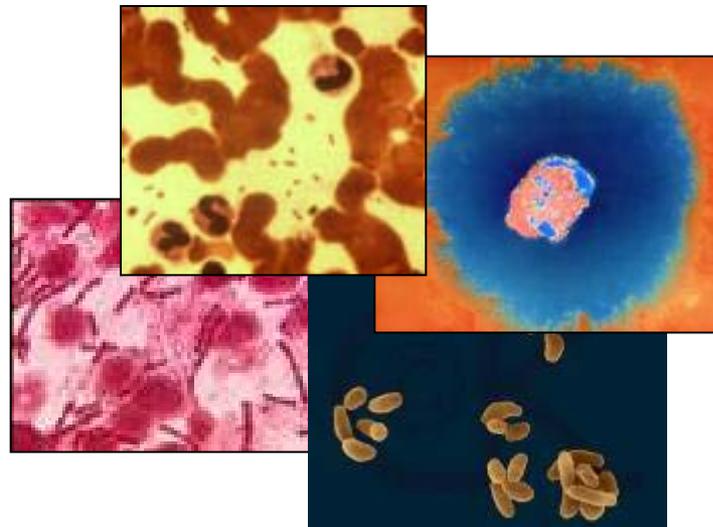


European Committee for Standardization  
Comité Européen de Normalisation  
Europäisches Komitee für Normung

- **World Health Organization Biorisk Reduction Program**

Addresses laboratory biosafety and biosecurity and infection control

For example, recently released laboratory handling guidance for H1N1





# Laboratory Biorisk Management Systems

- **Provide for the health and safety of laboratory workers and the environment**
- **Ensure the containment of hazardous infectious substances in laboratories**
- **Maintain citizens' confidence in the activities of the bioscience research community**
- **Increase transparency to investors in the biomedical and biotechnology industries**
- **Protect valuable research and commercial assets**
- **Reduce the risks of crime and terrorism**





# Conclusions

- **Protecting against risks of working with pathogens and toxins – including theft and misuse – should be a critical element of every modern bioscience laboratory**
- **Laboratory biosecurity should be based on intellectually substantive and scientifically credible methodologies – just like biosafety**
  - **Biosecurity Risk = Likelihood of targeting and successful theft and the resulting consequences**
  - **Mitigation strategies should be risk based and flexible**
- **Setting a new biorisk management paradigm is essential**



# Components of Biosecurity

