



# *Biosecurity Principles*



Biosafety and Biosecurity Awareness Training  
For Afghan and Pakistani Bioscientists  
December 7 – 9, 2009



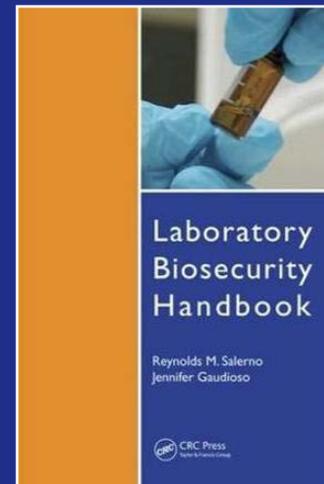
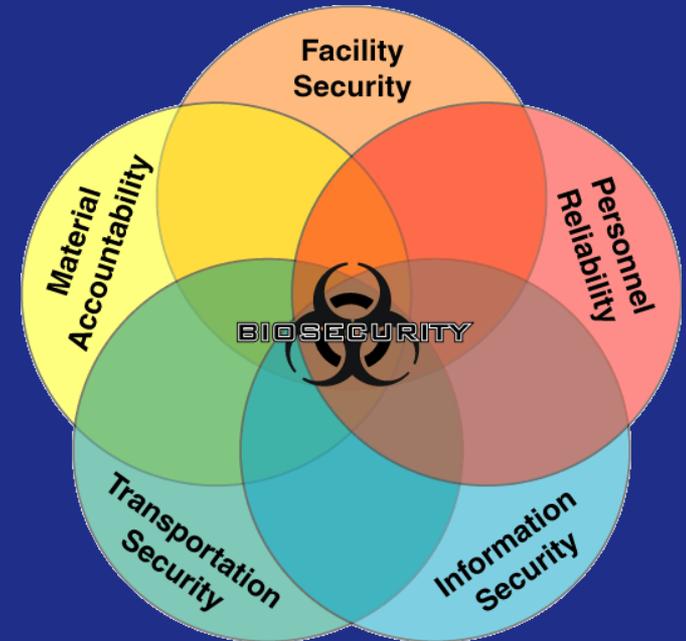
# What are the Key Components of Biosecurity?

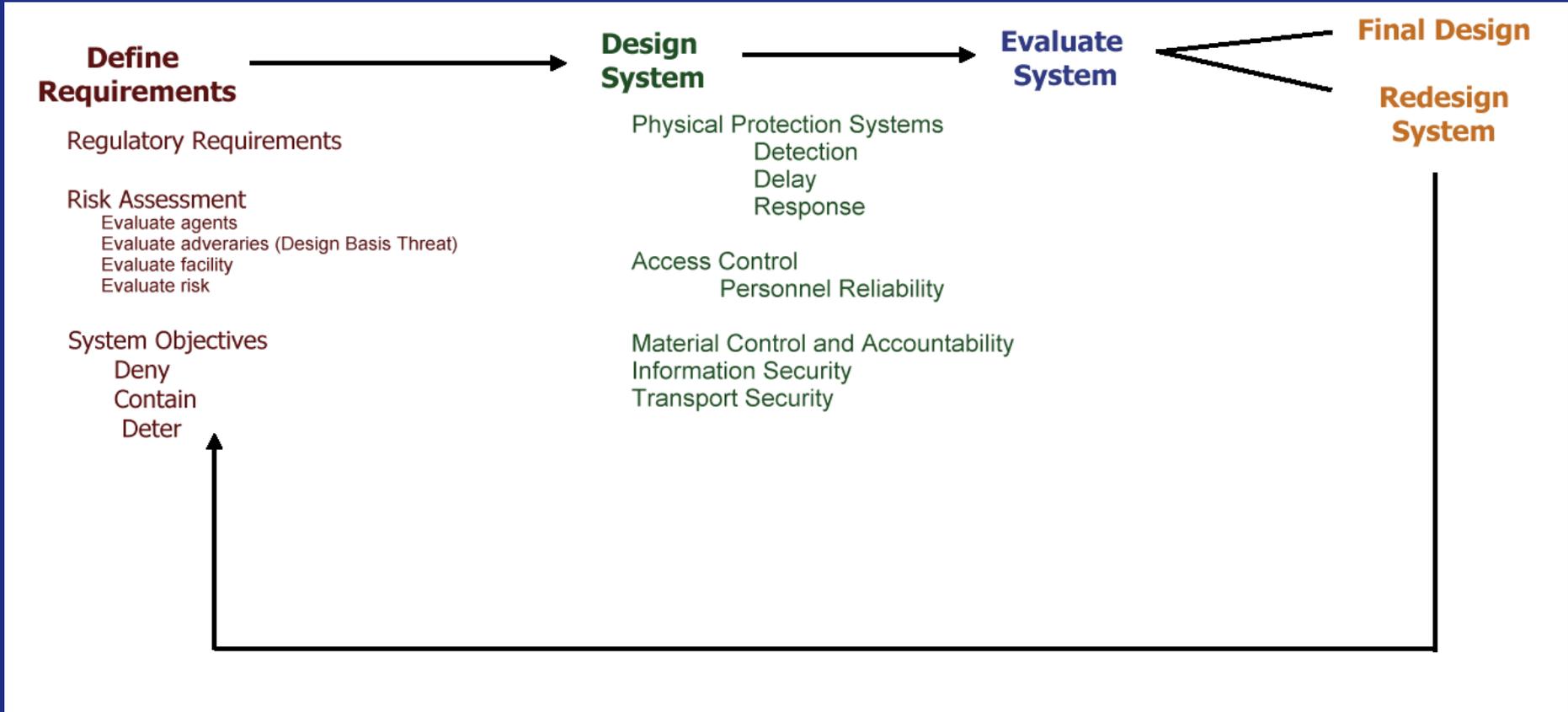
---



# 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**







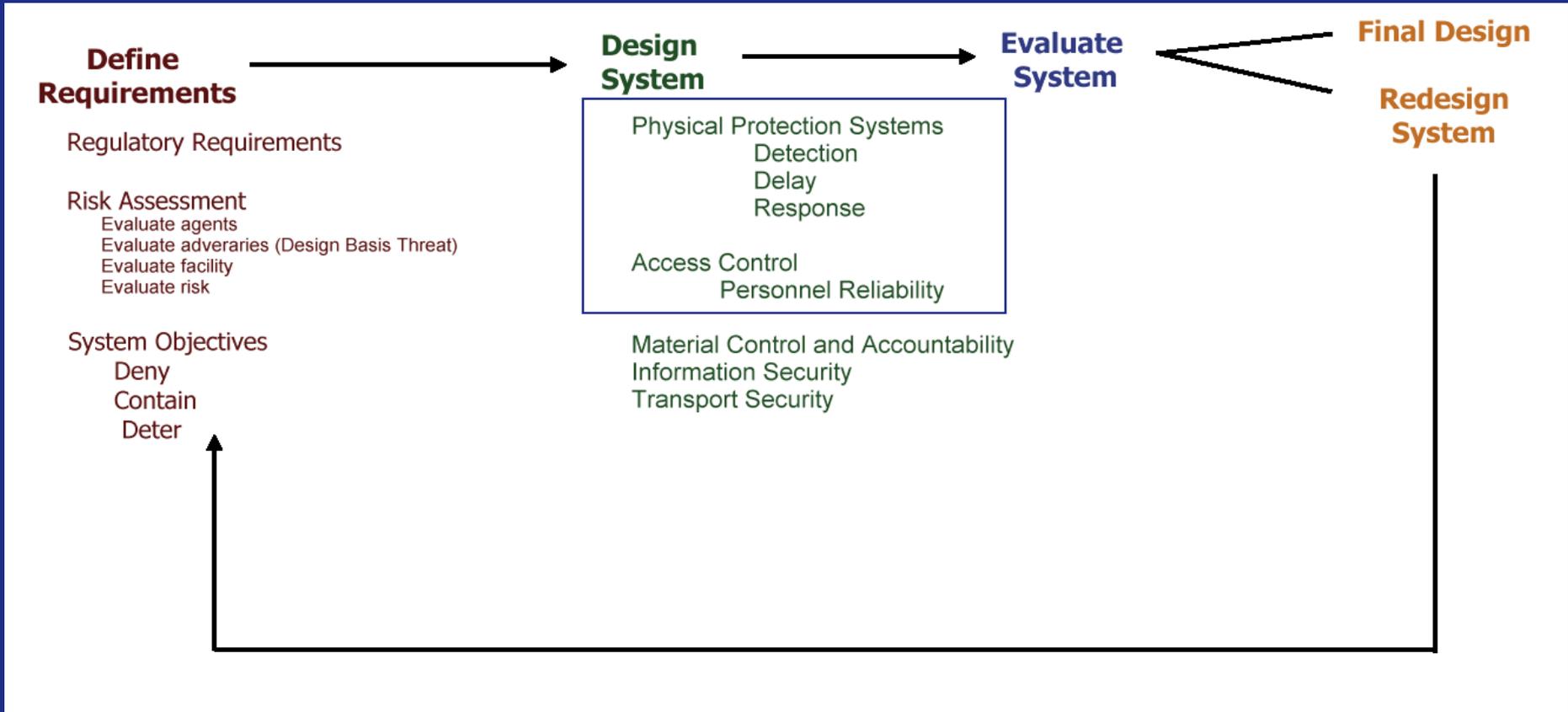
# Define System Objectives

- **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





- **What design objectives make sense for your facility?**
- **What design objectives would you want for a facility housing a novel dangerous pathogen like Small Pox?**
- **What objectives do you want for a diagnostic laboratory?**
- **Are they different?**





# Physical Protection Systems

- **Why is Physical Protection Important?**
- **How do you implement Physical Protection?**
  - What are the key components?



# Graded Protection for Bioscience Laboratories

- **Property Protection Areas**

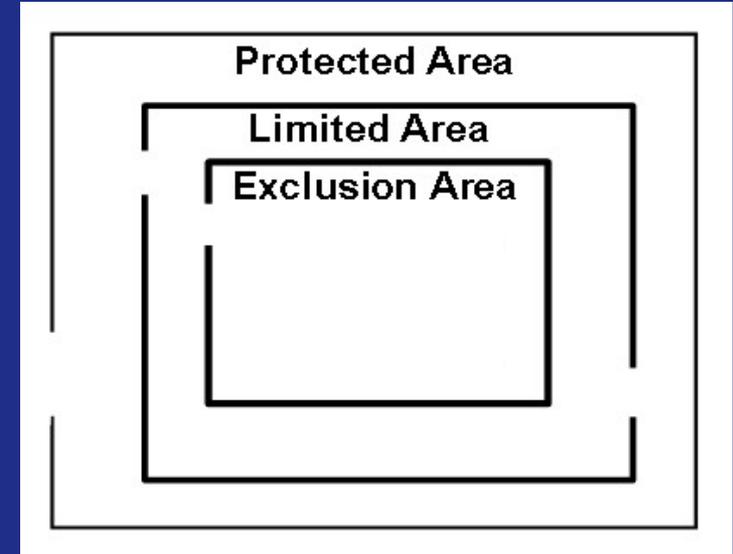
Low risk assets

- **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



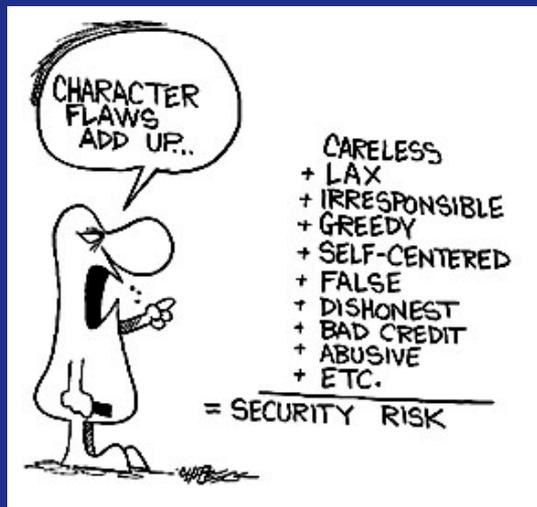
# Personnel Reliability

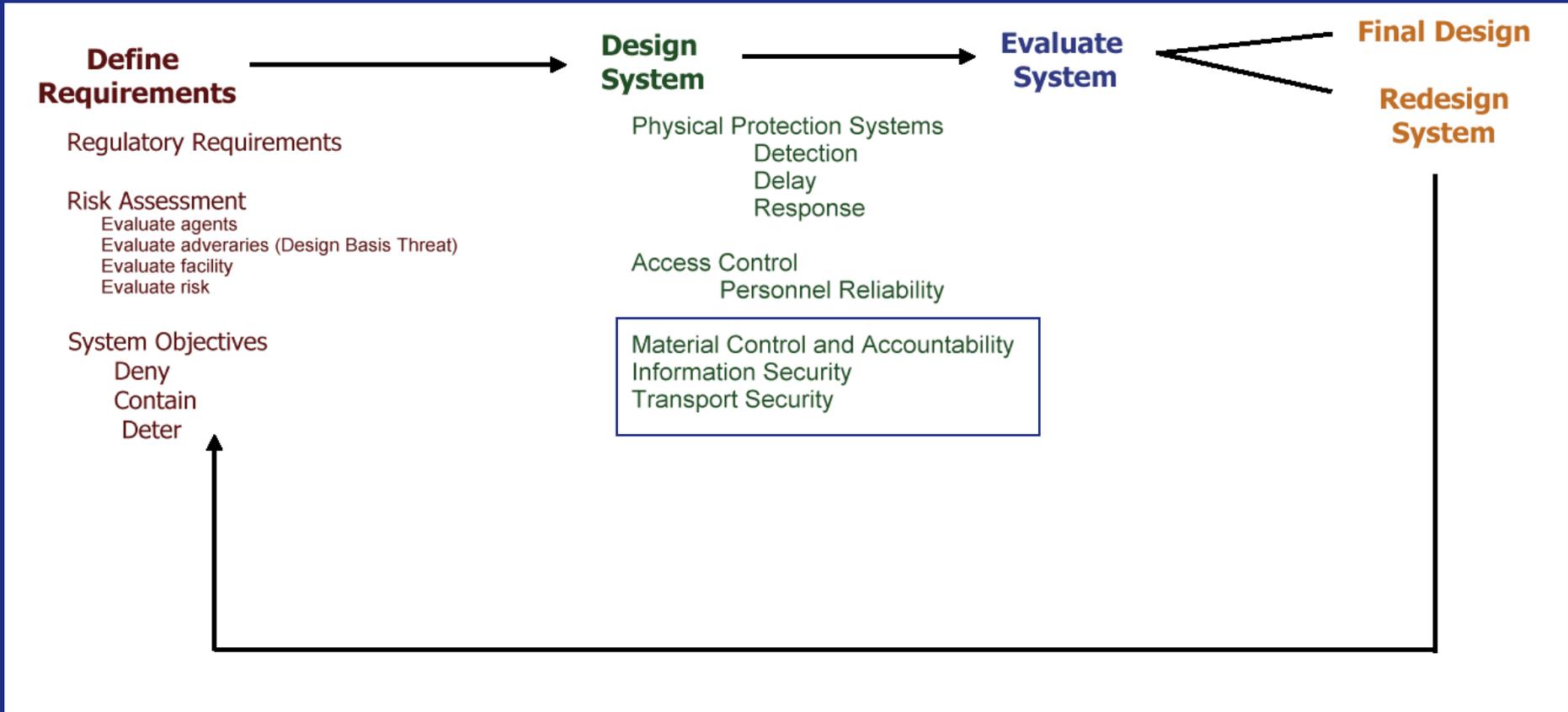
- Why is Personnel Reliability important?



# 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







# Material Control and Accountability

---

- Why do we care about material control?
- Why do we care about accountability?

# 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**





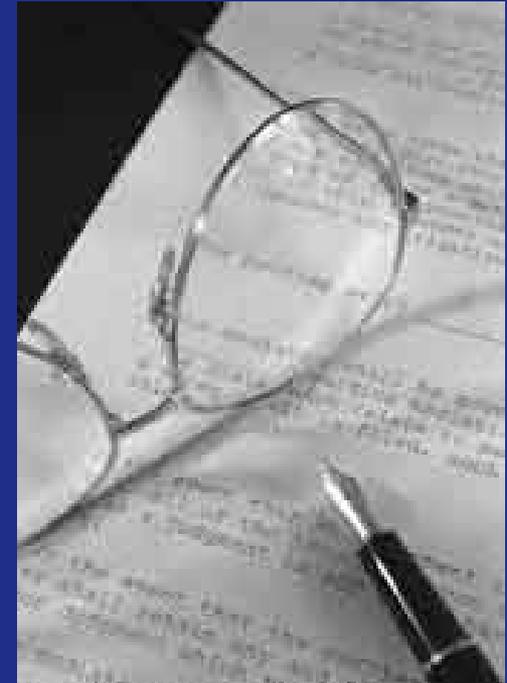
# Information Security

- Why do we care about information security?
- What information?
- How?



# 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





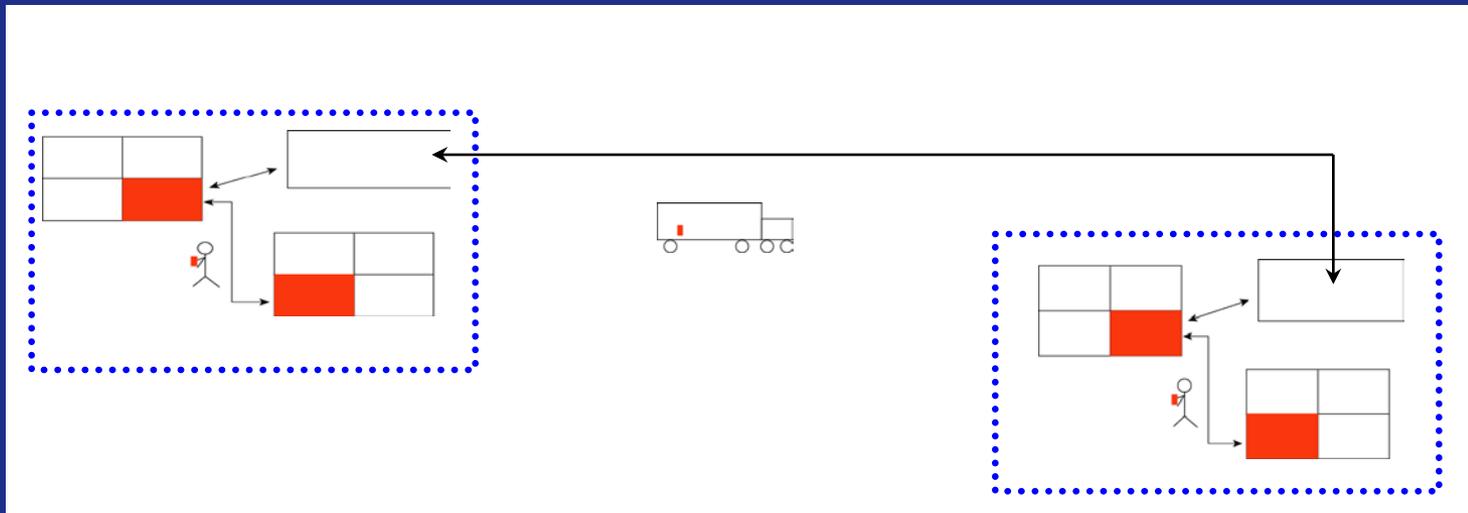
# Transport Security

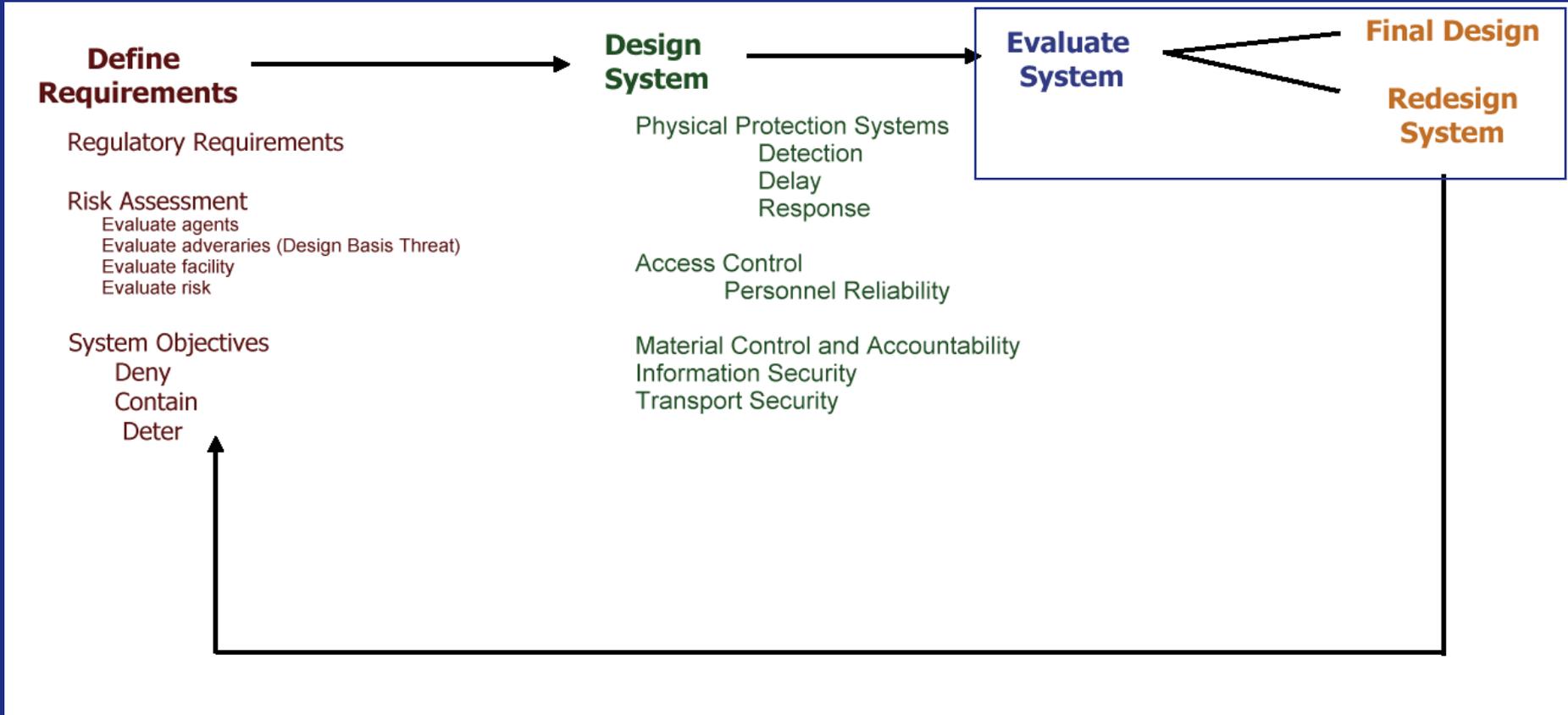
- Why is transport security important?
- Where should we think about transport security?



# 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







# 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**

