Approaches for a Unified Laboratory Biorisk Management Framework
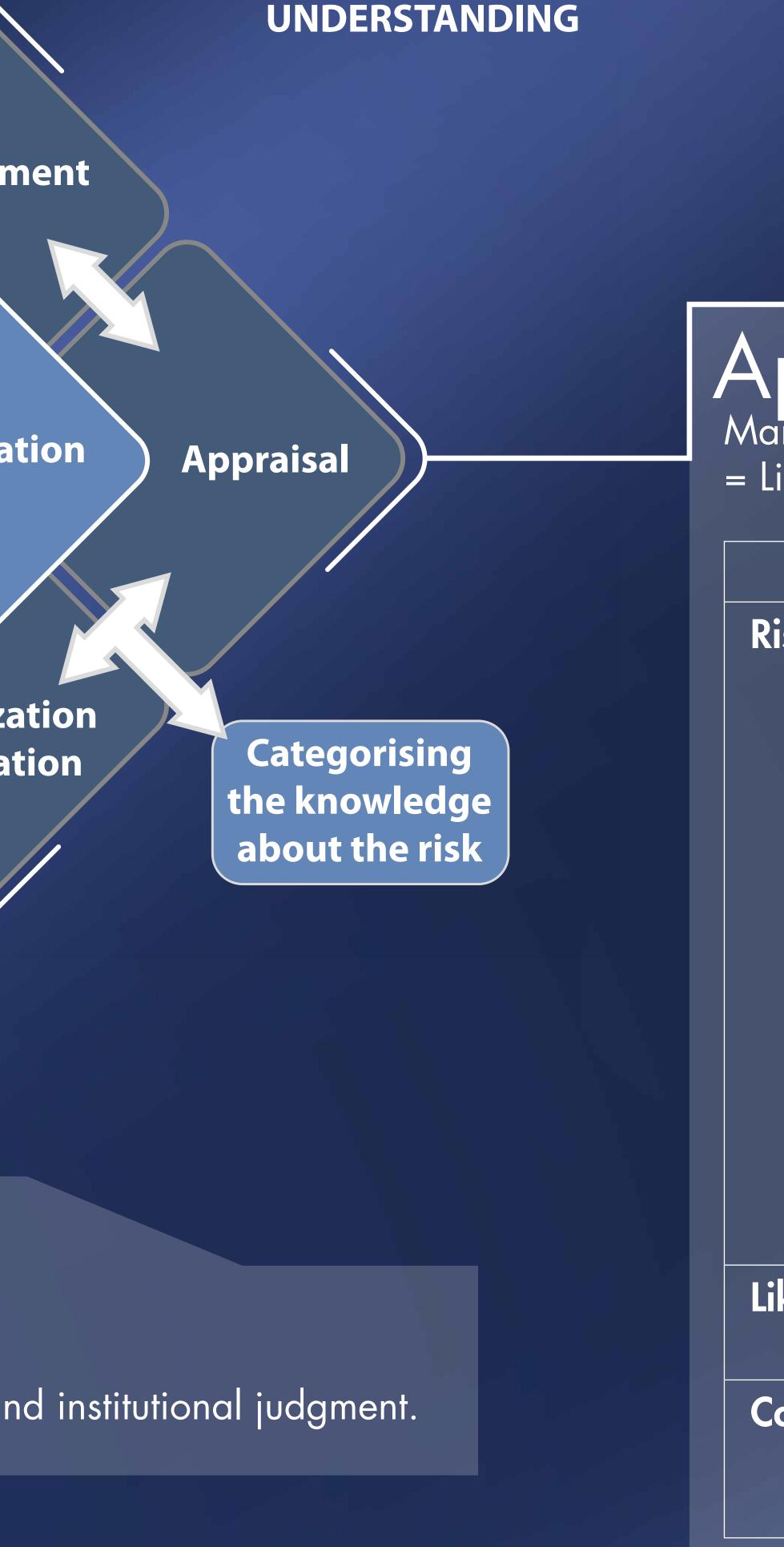
Jennifer Gaudioso, Susan Caskey, Reynolds Salerno - Sandia National Laboratories, Albuquerque, NM, USA

LouAnn Burnett - Vanderbilt University, Nashville, TN, USA

Erik Heegaard - Biosecurity Institute, Lyngby, Denmark

Jeffery Owens - Diversified Laboratory Sciences, Inc, Atlanta, GA, USA

Philippe Stroot - Xibios Biosafety Consulting, Tournai, Belgium

Communication:

Risk communication is at the heart of the risk governance framework and should be a centerpiece of any biorisk management program. Without denying the importance of common ways of communication, this report looked at the applicability of new communication tools to the different framework elements, including:
- Microblogging (Twitter, Identica)
- Blogging (Blogspot, WordPress.com)
- Wikis (Wikipedia, Intellipedia)
- Forums, online discussions, and e-mail list services (Yahoo! Groups, Google Groups)
- Document collaboration systems (SharePoint, Google Docs, Scribd)
- Tagging (Evidenced by Delicioius, Flickr, WordPress) and
- Social bookmarking (Delicious, Digg)
- Online rating systems (Amazon, Digg)
- Content management systems (Plone, Drupal)
- Social networking (Facebook, LinkedIn, Twitter)
- Photo sharing (Flickr)
- Podcasting and video-sharing (YouTube)
- Online distributed office applications (GoogleDocs)

Pre Assessment:

Biorisk cases:
- Under this project, 63 recent cases were analyzed and could be grouped into the following categories:
  - Laboratory exposure (actual or potential)
  - Unintentional release from facility
  - Theft
  - Inappropriate shipments
  - Inventory discrepancies
  - Unauthorized access
  - Unauthorized experiments
  - Inadequate biosafety measures
  - Inadequate biosecurity measures
  - Problems with documentation
  - Inadequate training
- All ultimately illustrating the importance of a robust biorisk management framework.

Biorisk drivers – what are the policy and operational drivers that might influence an institution's adoption of a biorisk management system:
Policy drivers identified:
- Financial concerns
- Ethics, corporate social responsibility
- Incidents
- Public demands, public image
- Technology advances
Operational drivers identified:
- Rules/regulations (national legislation)
- International treaties
- Guidance documents
- Financial concerns
- Customer demands
- Market policy

Management:

The lack or insufficiency of appropriate training and personnel reliability programs are two important gaps identified through this project and by others. This project looked at practices in other industries on these two topics.

Training:
Retention can be explained by classifying tasks into skill sets:
- Physical and speed-based skills appear to be retained longer than cognitive and accuracy-based skills.
- Closed-loop skills, which involve discrete responses that have a definite beginning and end, are retained longer than open-loop skills, which involve continuous, repeated responses that have no definite beginning or end.
Three issues to consider when determining optimal refresher training interval: 1. how frequently is the skill practiced in the workplace? 2. how susceptible is that type of skill to decay? 3. how much retraining is necessary to restore effectiveness?

Personnel Reliability Programs:
Like any risk mitigation measure, PRPs are not foolproof. However, they attempt to help us determine who is trustworthy. This project examined PRP programs from a range of industries (nuclear, aviation, finance, and healthcare) to better inform and inspire the discussion of PRPs among biosecurity practioners and to help us start identifying reasonable alternatives for biosecurity.

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

Measuring effectiveness of risk management system:
A variety of measures were examined, including management performance indicators, operational performance indicators, and biorisk status indicators.
- Analysis of performance indicators used in other industries (e.g. chemical)
- Ways to assess biorisk climate through questionnaires
- Behavior-based coaching processes
- Ways to strengthen incident reporting
  - Defining incident and level of risk
  - Notification and response protocol with risk-based tiers
  - Models for root cause analysis

Sustainability of biorisk management systems:
The study also aimed to articulate the processes, knowledge and skills that are required to ensure the sustainability of biological activities, both in planning for and building biocontainment facilities and in managing biorisk during operations.

DECIDING / UNDERSTANDING

Pre-Assessment — Communication — Appraisal — Management — Characterization and Evaluation

Categorising the knowledge about the risk

Characterization and Evaluation:

Not addressed in this project; left to national and institutional judgment.

Appraisal:

Many risks to be assessed independently although they may be best managed in a unified framework. Risk = Likelihood * Consequences

	Biosafety	Biosecurity

Risks	1. Risk to individuals performing direct manipulation to agent (in vitro and in vivo)
	 2. Risk to individuals working in same laboratory
	 3. Risk to persons within facility
	 4. Risk to community of primary exposure
	 5. Risk to community of secondary exposure
	 6. Risk to animal community of breach of containment
	 7. Risk to animal community of secondary exposure
		1. Risk that an agent is stolen from a facility and subsequently used to execute a bioterrorism attack
		   a. Risk to persons directly exposed
		   b. Risks to humans from secondary exposure
		   c. Risks to animals directly exposed
		   d. Risks to animals from secondary exposure
		   e. Risks to economy
		   f. Risks to facility
		 2. Risk that intellectual property is stolen (facility faces financial, operational, reduced market share impacts)
		 3. Risk that the facility is sabotaged (by issue extremists or to release pathogens)

Likelihood	Likelihood of infection * Likelihood of exposure	Likelihood of theft from a facility * Likelihood agent can be used as a weapon
Consequences	Disease impacts (direct and secondary exposure based on model)	Disease impacts (direct and secondary exposure) plus socioeconomic impacts