

Course Number: XXXX

Critical Infrastructure Protection: Risk Management

University of XXXXXXXX

Fall/Spring Semester 20XX

NAME OF SCHOOL:

DEPARTMENT:

PROFESSOR:

Telephone Number:

Office Location:

Office Hours:

Email:

Website:

COURSE DESCRIPTION/OVERVIEW:

This course provides an introduction to the policy, strategy, and practical application of risk management and risk analysis from an all-hazards perspective. It explores the strategic and operational context presented in the 2009 National Infrastructure Protection Plan (NIPP) and presents the challenges associated with managing security risks in general. The course promotes subject-matter understanding, critical analysis of analytic approaches, and proficiency in communicating information about risk analysis methods and findings in oral and written form. It also addresses the opportunities and challenges associated with other critical infrastructure competency areas, such as infrastructure-related public-private partnerships, information sharing, performance metrics, and decision support. The development of skills and knowledge will be promoted through readings, lectures, and class discussions, as well as exercised through papers and in-class presentations.

Risk management is both a foundational concept and an analytic discipline deeply ingrained in the conduct of critical infrastructure protection. It applies equally to all of the 18 infrastructure sectors identified in the NIPP. Conceptually, its application in critical infrastructure protection should be simple; by understanding the risks to critical infrastructures we can improve their protection from (and improve resilience to) harmful events. But to manage risks effectively, one must first be able to measure risks. This is where the simplicity of the concept of *risk management* and the complexity of *risk analysis* diverge. The underlying discipline of rigorous qualitative and quantitative analysis of security risks is a relatively recent and complex endeavor in security and critical infrastructure, the future direction of which is still the subject of deep study and debate. Learners will be challenged to understand this evolving situation and prepare

themselves to take part in it.

CREDITS CONFERRED: 3

PREREQUISITES: Introduction to Critical Infrastructure Protection and Resilience

Many forms of risk analysis contain mathematical expressions and/or statistical concepts. These will be discussed fully in class and through assigned readings and will be reflected in learner projects. While this course will not prepare learners to develop their own methodologies and advanced mathematical expressions for risk, successful learners should utilize the course to ensure that they leave prepared to read, understand, and articulate those most commonly used. Learners are advised to review basic algebra and statistics prior to the course if, in their own judgment, such review is needed.

LEARNER OUTCOMES/OBJECTIVES (AS MAPPED AGAINST DEPARTMENT OF HOMELAND SECURITY CRITICAL INFRASTRUCTURE CORE COMPETENCIES):

Risk management and analysis supports, and is supported by, most of the other core competencies of critical infrastructure. For example, when employed properly, risk analysis supports executive and managerial decision-making and justifies the creation and prioritization of programs and investments. It informs the selection of protective measures and mitigation strategies. Risk analysis is performed to provide the metrics to establish goals and objectives for programs, and it allows their reprioritization when those risks are reduced to an acceptable level. Finally, risk management provides the common framework and lexicon for thinking and communicating about critical infrastructure risks. This communication architecture enables effective information sharing and collaboration about risks between State, tribal, territorial, and local government officials, U.S. Department of Homeland Security (DHS) personnel, Sector-Specific Agencies (SSAs), and infrastructure owners and operators. Conversely, performing risk management well depends upon effective program management and information sharing among partners. Performing risk management also requires data collection to feed the analytic process, and must incorporate sector-specific expertise to drive practical and cost-effective reductions in risk within a given infrastructure sector.

Although the focus of this course is primarily risk management, this course is designed to enable learners to understand:

1. Risk analysis:

- Balancing the benefits, compromises, costs, and implications associated with proposed risk analysis models or tools
- Selecting the appropriate risk assessment techniques and models for the critical infrastructure assets, systems, and networks, as well as the decision requirements
- Using threat, vulnerability, consequence analysis information, and statistical data (when available) to calculate quantitative risk levels
- Understanding attributes used to define risk analysis in security vs. risk analysis in other areas (insurance, finance, engineering, etc)

- Understanding security analysis methods other than risk assessments

2. Protective measures and mitigation strategies:

- Using risk analysis to identify and compare the effectiveness of protective measures that address physical, cyber, and human risks
- Taking mitigation actions based on their assessed efficacy and efficiency in reducing risk strategies
- Understanding resilience as a means of risk management

3. Partnership building and networking:

- Understanding risk management as a collaborative endeavor between critical infrastructure partners and the importance of stakeholder participation
- Understanding risk analyst – threat analyst collaboration
- Using a common risk lexicon as an enabler to building common understanding

4. Information collection and reporting (information sharing):

- Understanding the intelligence analysis cycle
- Obtaining intelligence reporting and receipt of the threat data
- Collecting qualitative and quantitative data on threats, vulnerabilities, and consequences for natural and man-made hazards
- Inferring “threat” from intelligence sources, suspicious incidents, and other indicators
- Formulating intelligence data requests

5. Program management:

- Managing, timing, and scoping of risk analyses as management tasks
- Understanding time, data collection, availability, and cost as management factors
- Appreciating analytical risks (incorrect data, overconfidence, “paralysis by analysis,” uncertainty, and complexity)
- Achieving an “acceptable level of risk”

6. Metrics and program evaluation:

- Evaluating assessment results
- Determining which critical infrastructure should be given priority and which alternatives represent the best options based on risk reduction
- Recognizing when new or additional data are needed to evaluate threats, vulnerabilities, and consequences

7. Sector-specific technical and tactical expertise:

- Assessing risks to physical assets
- Assessing logical assets, networks, and intangible assets
- Understanding dependencies and interdependencies

DELIVERY METHOD/COURSE REQUIREMENTS:

Learners will be taught through a combination of assigned readings, lectures, group discussion, research papers, and an in-class oral presentation. The learner will be taught, independently and through collaboration with others, a body of knowledge pertaining to risk analysis and risk management. Learners will share this knowledge with fellow learners and faculty via class discussions, written papers, and oral presentations.

The assigned course readings include a variety of resources, such as authoritative readings (legislation, executive orders, policies, plans, and strategies), implementation readings (government products that are responsive or attempt to fulfill the requirements of authoritative documents), and external reviews (U.S. Government Accountability Office, Congressional Research Service, etc.). Learners are expected to familiarize themselves with the assigned topic and readings before class and should be prepared to discuss and debate them critically as well as analyze them for biases and multiple perspectives.

GENERAL COURSE REQUIREMENTS:

1. Class attendance is both important and required. If, due to an emergency, you will not be in class, you must contact your instructor via phone or email. Learners with more than two absences may drop a letter grade or lose course credit.
2. It is expected that assignments will be turned in on time (the beginning of the class in which they are due). However, it is recognized that learners occasionally have serious problems that prevent work completion. If such a dilemma arises, please speak to the instructor in a timely fashion.
3. The completion of all readings assigned for the course is assumed. Since class will be structured around discussion and small group activities, it is critical for you to keep up with the readings and to participate in class.
4. All beepers and cell phones should be turned off before class begins.

RESEARCH PROJECTS AND PRESENTATIONS:

1. Research Paper/Oral Presentation (40%):

Each learner will prepare a 20 to 25 page (double-spaced) research paper on a relevant topic of interest in the area of risk management and its application within the field of critical infrastructure protection. The paper should clearly state its hypothesis or propose a solution to a known issue or problem. The paper should strive to support the hypothesis or solution with authoritative reports, articles, interviews, or other data.

Each learner will present his/her research topic (no more than 15 minutes in length) to the class during **Lessons 13-14**. Following the presentation, learners will have 5 additional

minutes for questions. The presentation format will mirror that of the research paper. Research papers will be submitted on the last day of class, and will incorporate learner and instructor feedback from the oral classroom presentation.

Prior approval of the topic for the research paper is required. Learners must submit a one-paragraph written description of their proposed topic for approval no later than the beginning of class on **Lesson 3**.

2. Individual Methodology Analysis Paper/Presentation (30%):

Each learner will be expected to identify, critically analyze, and prepare a 10 to 12 page paper (double-spaced) on a security analysis method (i.e., combining the three factors of risk: consequences, threats, and vulnerabilities). If needed, the instructor can assist learners in identifying suitable analytic methods. However, learners may first want to review SARMApedia at <http://sarma-wiki.org/index.php?title=Category:Methodologies> for a partial listing of these methods. Additional research and documentation will be required.

The instructor reserves the right to limit duplication of methodologies. Therefore, learners are required to submit their proposed method for study and at least one alternate choice to the instructor no later than the end of the **Lesson 8**.

Each paper will be turned-in with appropriate methodology documentation — typically the documentation written by its creators or proponents — unless by prior arrangement with the instructor. Each learner’s paper will be presented orally to the class at a pre-arranged time during the semester.

Your analysis of each analytic method should address all of the aspects of risk analysis to be covered in the course. These include:

- Origin, intended purpose, intended audience, and intended decisions
- Description of the methodology’s major elements and attributes
- Characterization of the method’s quantification schema (or lack thereof)
- Methods of aggregating consequence, threat, and vulnerability into “risk”
- Treatment of man-made and natural hazards
- Treatment of risk at sector and geographic levels
- Strengths of the approach
- Weaknesses of the approach
- Your recommendations for method improvement

EXPECTATIONS FOR PARTICIPATION (30%):

Participation includes coming to class prepared, participating fully in class discussion, and completing individual and group assignments consistent with your abilities and level of experience.

INCORPORATION OF FEEDBACK:

The course instructor will provide multiple opportunities for learners to provide constructive feedback over the period of the course. These may be in the form of group sessions or one-on-one sessions with the instructor. Learners will be afforded the opportunity to complete in-class evaluations at the end of the course. On-line feedback is also encouraged throughout the course.

COURSE TEXTBOOKS:

The following textbook is identified as the primary textbook reading for the course. The textbook will be supplemented by additional readings accessible on-line, with website addresses provided in the lesson description section that follows.

Julian Talbot and Miles Jakeman, *Security Risk Management Body of Knowledge (SRMBOK)*, (Hoboken, New Jersey: John Wiley and Sons, Inc., 2009).

GRADING SCALE: SCHOOL POLICY DEPENDENT

COURSE SCHEDULE

LESSON 1 TOPIC: SECURITY RISK AS AN ANALYTIC DISCIPLINE

1. Lesson Goals/Objectives:

- Become familiar with the scope of the course, administrative requirements, instructional methodology, evaluation criteria, and feedback processes
- Learn the risk analysis and risk management sets of “triplets”
- Understand security risk as a subset of all risk
- Gain familiarity with the basic terminology of risk management
- Identify the factors of security risk (threat, vulnerability, and consequence)
- Learn how to read the mathematical representation of a risk analysis
- Discuss non-risk security analysis methods frequently used
- Understand how critical infrastructure protection decisions are supported by security risk analysis
- Explore the continuum of security risk, from prevention and protection to response and recovery
- Examine the levels at which risk analysis is used in critical infrastructure protection (strategic, tactical, policy, operational, etc.)

2. Discussion Topics:

- What are the differences between threat and vulnerability?
- Identify threats, vulnerabilities, and consequences of a series of terrorist attacks and natural hazard scenarios. Compare and contrast man-made events (both malicious incidents and accidents) and natural hazards.
- What critical infrastructure protection -related decisions might a risk assessment support? Examples include protective measures, incident management, facilities placement, operations security (OPSEC), continuity of operations (COOP), and response capabilities.
- What is acceptable risk? How does acceptable risk differ among stakeholders?
- How does risk analysis change depending on the decision-maker? Describe one scenario and explain how different decision-makers (e.g., a facility manager, a mayor, a governor, a public health official, Federal infrastructure protection officials, etc.) would have different needs for inputs and outputs.
- What are the benefits of risk-based approaches? When might an examination of one risk factor be appropriate for decision-making? When might it lead to poor results?
- How do the international, Government Accountability Office (GAO), and NIPP and Integrated Risk Management Framework (IRMF) risk frameworks differ?
- Which risk analysis methods are participants familiar? Who uses them?

3. Required Reading:

SRMBOK, Chapter 1: Introduction and Overview; Chapter 4: SRMBOK Framework

National Research Council, Committee on Risk Characterization, *Understanding Risk:*

Informing Decisions in a Democratic Society, P. C. Stern and H. V. Fineberg (eds.), Washington, D.C.: National Academy Press, 1996.
<http://books.nap.edu/openbook.php?isbn=030905396X>.

Stanley Kaplan and B. John Garrick, “On the Quantitative Definition of Risk,” *Risk Analysis* 1(1), 1981. <http://josiah.berkeley.edu/2007Fall/NE275/CourseReader/3.pdf>.

Yacov Haimes, “Total Risk Management,” *Risk Analysis* 11(2), 2006.

U.S. Department of Homeland Security, *Risk Management Fundamentals: Homeland Security Risk Management Doctrine*, April 2011.

U.S. Department of Homeland Security, *National Infrastructure Protection Plan*. Executive Summary, Chapter 3. 2009.
http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

4. Additional Recommended Reading:

U.S. Department of Homeland Security, DHS Steering Committee, DHS Risk Lexicon, 2010. <http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf>.

LESSON 2 TOPIC: BASIC APPROACHES AND MODELS

1. Lesson Goals/Objectives:

- Understand the different categories of models (conceptual, formal, and computational)
- Identify the basic approaches to risk analysis (qualitative, quantitative, and semi-quantitative)
- Comprehend the differences among nominal, ordinal, interval, and ratio scales and the differences between natural and constructed scales
- Understand the considerations that influence assessment types (data availability, timeframe required for analytic results, needs of decision-maker, available resources, etc.)

2. Discussion Topics:

- What are the advantages and disadvantages of qualitative, quantitative, and semi-quantitative models?
- What makes a good ordinal scale? What are some common mistakes in constructing scales?
- How does the selection of scale affect the risk analysis?

3. Required Reading:

SRMBOK, Chapter 5: Practice Areas.

National Research Council, Committee on Risk Characterization, *Understanding Risk: Informing Decisions in a Democratic Society*, P. C. Stern and H. V. Fineberg (eds.), Chapter 2: Judgment in the Risk Decision Process, Washington, D.C.: National Academy Press, 1996.

Joshua M. Epstein, "Why Model?" July 2008.

<http://www.mit.edu/~scienceprogram/Materials/Monday%20Materials/WhyModel.pdf>.

Richard Pariseau and Ivar Oswald, "Using Data Types and Scales for Analysis and Decision Making," *Acquisition Review Quarterly*, Spring 1994. <http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA296380>.

U.S. Department of Defense, "Standard Practice for System Safety," MIL-STD-882D, February 2000. <http://www.acq.osd.mil/atptf/policy/documents/MILSTD882D.pdf>.

U.S. General Accounting Office, "Threat and Risk Assessments Can Help Prioritize and Target Program Investments," April 1998.

<http://www.loyola.edu/departments/academics/political-science/strategic-intelligence/intel/nsiad98-89.pdf>.

4. Recommended Reading:

System Safety Society, "System Safety: A Science and Technology Primer," April 2002.

http://www.system-safety.org/resources/SS_primer_4_02.pdf.

Ronald MacKenzie and Mary E. Charlson, "Standards for the Use of Ordinal Scales in Clinical Trials," *British Medical Journal*, 292(4), January 1986.

LESSON 3 TOPIC: SCENARIO GENERATION

1. Lesson Goals/Objectives:

- Understand the importance of establishing the context for a risk assessment
- Become familiar with how to set goals and objectives at the outset of a risk management project
- Identify types of critical infrastructure assets that may require protection (e.g., people, physical items, functions, cyber, data, reputation, etc.)
- Understand methods for screening a set of assets for criticality, including multi-attribute utility theory
- Understand the definition of a scenario (a hazard, an entity impacted by that hazard, and associated conditions, including consequences when appropriate) and how to evaluate scenarios for completeness and appropriateness (including internal consistency and documentation of explicit assumptions and variables)
- Discuss and utilize multiple methods of generating scenarios
- Discuss approaches to screening or filtering scenarios (e.g., alignment with an adversary's goals, degree of public acceptance of risk, feasibility, and plausibility)
- Understand the fundamental role that scenario generation plays in producing comparable risk levels

2. Discussion Topics:

- How does the interaction of the decision-maker, the hazard types, and the assets influence the context and parameters for a risk assessment?
- How should a decision-maker's missions, responsibilities, and authorities influence the inputs and outputs of a risk model?
- How does the context of an assessment influence the scope of the scenarios considered?
- How do the number of asset types and the number of analysts involved in the process influence scenario generation?
- Are all scenarios appropriate for all sectors?
- How might an analyst assign weights to attributes in a process with multiple decision-makers with different perceptions of relative importance of those attributes?
- How does the level of the risk analysis (e.g., strategic, tactical, policy, or operational) influence the need for detail in a scenario?
- When is it appropriate to use a worst-case scenario? How do you define "worst"? How might you limit severity of a scenario to a reasonable extent?

3. Required Reading:

SRMBOK, Chapter 10: Asset Areas; Chapter 6: Strategic Knowledge Areas (6.2.4) Criticality.

National Research Council, Committee on Risk Characterization, *Understanding Risk: Informing Decisions in a Democratic Society*, P. C. Stern and H. V. Fineberg (eds.), Chapter 3: Deliberation, Washington, D.C.: National Academy Press, 1996.

M. Granger Morgan, H. Keith Florig, Michael L. DeKay, and Paul Fischbeck, "Categorizing Risks for Risk Ranking," *Risk Analysis*, 2000.

Yacov Y. Haimes, Stan Kaplan, and James H. Lambert, "Risk Filtering, Ranking, and Management Framework Using Hierarchical Holographic Modeling," *Risk Analysis*, 2002.

http://lyle.smu.edu/emis/cmmi5/Ibarra/DeskTop/White_Papers/Risk_Analysis/Risk_RFR_M.pdf.

National Research Council, "Technical Input on the National Institutes of Health's Draft Supplementary Risk Assessments and Site Suitability Analyses for the National Emerging Infectious Diseases Laboratory, Boston University," 2007. Free Download.

4. Recommended Additional Reading:

U.S. Federal Emergency Management Association, "Using HAZUS-MH for Risk Assessment How-To Guide," Step 1: Identify Hazards, FEMA 433, 2004.

<http://www.fema.gov/library/viewRecord.do?id=1985>.

Faisal Khan, "Use Maximum-Credible Accident Scenarios for Realistic and Reliable Risk Assessment," *Chemical Engineering Progress Magazine*, November 2001.

http://findarticles.com/p/articles/mi_qa5350/is_200111/ai_n21481028/.

Philip van Notten, "Scenario Development: A Typology of Approaches," 2006.

<http://www.oecd.org/dataoecd/27/38/37246431.pdf>.

Congressional Research Service, "What Makes Infrastructure Critical"? August 30, 2002.

http://www.libertysecurity.org/IMG/pdf/CRS_Report_-_What_makes_an_Infrastructure_Critical_-_30.08.2002.pdf.

LESSON 4 TOPIC: THREAT ANALYSIS

1. Lesson Goals/Objectives:

- Understand the definition of threat in the context of critical infrastructure protection security risk
- Become familiar with the ontology of intentional man-made threats and its components (intent, capability, and opportunity)
- Understand the considerations for estimating natural hazard threats
- Understand the types of threat assessments and the roles they play in various critical infrastructure protection activities (e.g., strategic assessments, tactical assessments, indications and warning, detection, attack assessment, and damage assessment)
- Identify potential sources for threat information
- Understand methods of qualitatively comparing and quantifying threat (frequency, probability of attack, and strength of indicators)
- Understand alternate approaches to exploring threat, beyond history, precedent, and intelligence (e.g., red cell analysis, game theory, role playing, etc.)

2. Discussion Topics:

- How does threat differ in relation to the various types of terrorist groups on the domestic and international scene? Compare international terrorist groups with environmental extremists. Consider attack methods, potential targets, and intended results.
- To what extent does past frequency of natural hazards contribute to understanding probability for planning? How much priority should an emergency management office place on a very rare, catastrophic hazard? On an unprecedented hazard?
- Compare and contrast strategic threat and tactical threat (e.g., historical crime data vice current string of robberies).
- How might threat analysis, especially warning, influence risk?
- Compare the threat assessment for a scenario (e.g., terrorist attack on mass transit using explosives) based on considerations of frequency, probability of attack, and strength of indicators. When is frequency valid? When is Bayesian probability a useful approach for threat analysis?
- What are the roles of the DHS Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) and State and local fusion centers in identifying threats to potential targets?
- How would a strategic threat change into a tactical threat upon receipt of a warning?

3. Required Reading:

SRMBOK, Chapter 6: Strategic Knowledge Areas (6.2.2) Threat.

National Research Council, Committee on Risk Characterization, *Understanding Risk: Informing Decisions in a Democratic Society*, P. C. Stern and H. V. Fineberg (eds.), Chapter 4: Analysis, Washington, D.C.: National Academy Press, 1996.

Homeland Security Institute, “Risk Analysis and Intelligence Communities Collaborative Framework,” April 2009. <http://www.homelandsecurity.org/hsireports/Risk-Intel%20Collaboration%20Final%20Report.pdf>.

George Mason University, *Critical Infrastructure Protection: Elements of Risk*, Chapter 2 “Intelligence Analysis for Strategic Risk Assessments,” 2007. http://www.steelcityre.com/documents/RiskMonograph_1207.pdf.

Jessica McLaughlin and M. Elisabeth Paté-Cornell, “A Bayesian Approach to Iraq’s Nuclear Program Intelligence Analysis: A Hypothetical Example,” presentation at the 2005 International Conference on Intelligence Analysis, McLean, VA, May 2, 2005. https://analysis.mitre.org/proceedings/Final_Papers_Files/85_Camera_Ready_Paper.pdf.

U.S. Department of Defense, “Joint Tactics, Techniques, and Procedures for Antiterrorism,” Joint Pub 3-07.2, 1998. http://www.bits.de/NRANEU/others/jp-doctrine/jp3_07_2rsd.pdf.

4. Recommended Additional Reading:

Alan N. Steinberg, “An Approach to Threat Assessment,” presentation at 7th International Conference on Information Fusion (FUSION), 2005. <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=01592001>.

U.S. General Accounting Office, “Combating Terrorism: Need for Comprehensive Threat and Risk Assessments of Chemical and Biological Attacks,” GAO/NSIAD-99-163, September 1999. <http://www.loyola.edu/departments/academics/political-science/strategic-intelligence/intel/nsiad99-163.pdf>.

Winterfeldt and Rosoff, “A Risk and Economic Analysis of Dirty Bomb Attacks on the Ports of Los Angeles and Long Beach,” *Risk Analysis*, 27 (3), 2007. <http://www-bcf.usc.edu/~winterfe/A%20Risk%20and%20Economic%20Analysis%20of%20Dirty%20Bomb%20Attacks%20on%20the%20ports%20of%20Los%20Angeles%20and%20Long%20Beach.pdf>.

U.S. Federal Emergency Management Association, “Using HAZUS-MH for Risk Assessment How-To Guide,” Step 2: Profile Hazards, FEMA 433, 2004. <http://www.fema.gov/library/viewRecord.do?id=1985>.

LESSON 5 TOPIC: VULNERABILITY ASSESSMENT

1. Lesson Goals/Objectives:

- Understand the definition of vulnerability in the context of critical infrastructure protection security risk
- Understand the importance of the risk assessment context when assessing vulnerability
- Identify countermeasures that reduce vulnerability to natural hazards
- Identify considerations in perimeter security (deter, detect, delay, and deny)
- Understand internal and external factors that contribute to vulnerability
- Identify approaches to limiting an adversary's opportunity to attack
- Understand cyber vulnerabilities and the role they play in physical and cyber incidents
- Understand the human factors involved in countermeasure effectiveness
- Understand methods of qualitatively comparing and quantifying vulnerability (probability, event trees, fault trees, minimal cut sets, checklists, and judgments)

2. Discussion Topics:

- Under what circumstances might deterrence work to limit terrorism? To which threat types does deterrence apply the most or least? Does deterrence work in the cyber environment?
- What role does technology play in security countermeasures? What other elements are involved in effective implementation?
- How do critical infrastructure dependencies and interdependencies complicate the vulnerability assessment process?
- What do we mean by the ability to withstand an attack? How might that consideration alter the focus of a risk assessment?
- How might co-location affect vulnerability?
- To what extent does the vulnerability or resilience of a population affect the risk associated with critical infrastructure?
- When is it most useful for an organization to examine its vulnerabilities relative to others in a similar sector of infrastructure? When is it most useful to examine its vulnerabilities relative only to each other?

3. Required Reading:

SRMBOK, Chapter 6: Strategic Knowledge Areas (6.2.3) Vulnerability .

Geoffrey S. French and David Gootzit, "Defining and Assessing Vulnerability of Infrastructure to Terrorist Attack," *Vulnerability, Uncertainty, and Risk: Analysis, Modeling, and Management: Proceedings of the ICVRAM 2011 and ISUMA 2011 Conferences*, 2011.

http://ascelibrary.org/proceedings/resource/2/ascecp/400/41170/95_1?isAuthorized=no.

Yacov Y. Haimes, "On the Definition of Vulnerabilities in Measuring Risks to Infrastructures," *Risk Analysis*, 26 (2), 2006, 293–296.

James Reason, "Human Error: Models and Management," *British Medical Journal*, March 2000.
http://www.paediatricchairs.ca/safety_curriculum/domain5_docs/HumanErrorReason.pdf

U.S. Department of Defense, "Military Standard: Procedures for Performing a Failure Mode, Effects and Criticality Analysis," MIL-STD-1629A, November 24, 1980.
<http://sre.org/pubs/Mil-Std-1629A.pdf>.

4. Recommended Additional Reading:

Congressional Research Service Report, "Vulnerability of Concentrated Critical Infrastructure: Background and Policy Options," 2008.
<http://www.fas.org/sgp/crs/homsec/RL33206.pdf>.

Cutter, S.L., Boruff, B.J., & Shirley, W.L. "Social Vulnerability to Environmental Hazards," *Social Science Quarterly*, 84 (2), 2003, 242–261.
<http://www.colorado.edu/hazards/resources/socy4037/Cutter%20%20%20Social%20vulnerability%20to%20environmental%20hazards.pdf>.

U.S. Government Accountability Office, "Biosafety Laboratories: BSL-4 Laboratories Improved Perimeter Security Despite Limited Action by CDC," GAO-09-851, 2009.
<http://www.gao.gov/new.items/d09851.pdf>.

William L. McGill, Bilal M. Ayyub, and Mark Kaminskiy, "Risk Analysis for Critical Asset Protection," *Risk Analysis*, 27 (5), 2007, 1265–1281.

Kansas Water Office, "Public Water Supplier Drought Vulnerability Assessment," 2007.
http://www.kwo.org/reports%20&%20publications/drought/Rpt_pws_drought_assessment_FINAL_032307_twl.pdf.

LESSON 6 TOPIC: LIKELIHOOD ESTIMATION

1. Lesson Goals/Objectives:

- Understand the interactions among threat, vulnerability, and consequences
- Understand qualitative methods for integrating threat and vulnerability
- Become familiar with the ways that some existing models quantify and combine threat and vulnerability
- Understand conditional probabilities, event trees, and other approaches to probabilistic likelihood estimation
- Understand logical combinations of threat and vulnerability and methods of quantifying likelihood levels
- Become familiar with cases that present complex interactions among threat, vulnerability, and consequence (such as cascading effects, multi-staged attacks, biological events, and natural hazards with effects over time)

2. Discussion Topics:

- How does warning affect the *risk* from natural hazards? How does warning affect the *vulnerability* from a terrorist attack? How might it affect the *threat*?
- Do terrorist groups only attack soft targets?
- How are biological events detected? What actions can limit vulnerability or consequence?
- How are biological events and cyber events similar? How are they different?
- How do infrastructure dependencies affect response and recovery? How does social vulnerability affect response and recovery?

3. Required Reading:

Eric G. Little and Galina L. Rogova, "An Ontological Analysis of Threat and Vulnerability," in Proceedings of the FUSION 2006-9th International Conference on Multisource Information Fusion, July 10-13, Florence, Italy, 2006.

Rinaldi, Peerenbloom and Kelly, "Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies," 2001.

<http://www.ce.cmu.edu/~hsm/im2004/readings/CII-Rinaldi.pdf>.

C.G. Newhall and R. P. Hoblitt, "Constructing Event Trees for Volcanic Crises," *Bulletin of Volcanology*, 64, 2002, 3-20.

<http://earthweb.ess.washington.edu/lnk/ess-462/reading/prob-tree-final.pdf>.

LESSON 7 TOPIC: CONSEQUENCE ASSESSMENT

1. Lesson Goals/Objectives:

- Understand the definition of consequence in the context of critical infrastructure protection security risk
- Identify the categories of critical infrastructure–related consequences (i.e., human health, economic costs, mission disruption, and psychological or behavioral impacts)
- Understand how to determine which consequences to assess
- Understand how to determine units of measurement and valuation scales
- Understand the various sources for consequence assessment (e.g., historical examples, expert judgments, input–output models, surveys, simulations, etc.)
- Understand the differences between direct and indirect consequences
- Become familiar with willingness-to-pay models, value of a statistical life, and other methods of assigning monetary values
- Become familiar with multi-attribute utility theory, constructed scales, and other methods of assigning a consequence index number
- Become familiar with the ways that some existing models quantify consequence

2. Discussion Topics:

- What is the benefit of having all consequence measured in dollars? What are the limitations?
- Why are there different values for a statistical life?
- What is the benefit of considering psychological impacts of a terrorist event? What are the limitations with respect to critical infrastructures?
- What is the benefit of considering the loss of public morale if a national monument or icon was attacked and destroyed? Is the loss of morale the same as the loss of confidence in government?
- Why is it important to assess mission disruption and degradation?
- Why would a model include or exclude injuries and illness? Under what circumstances should a model distinguish between prompt versus delayed deaths? Why would a model include estimates of the number of “worried well”?
- How should a company value data loss? How should the government value private-sector loss of data?
- What are the differences in kind or magnitude between consequences borne by an individual company and those borne by the government?
- What consequences can a cyber attack on critical infrastructure have?

3. Required Reading:

Baruch Fischhoff, Stephen R. Watson, and Chris Hope, “Defining Risk,” *Policy Sciences*, 1984. <http://sds.hss.cmu.edu/media/pdfs/fischhoff/DefiningRisk.pdf>.

The Infrastructure Security Partnership (TISP), “Regional Disaster Resilience: A Guide for Developing an Action Plan,” Reston, Virginia: American Society of Civil Engineers, 2006. <http://www.tisp.org/index.cfm?cdid=10962&pid=10261>.

U.S. Federal Emergency Management Association, “Using HAZUS-MH for Risk Assessment How-To Guide,” FEMA 433, Step 4: Estimate Losses, 2004.
<http://www.fema.gov/library/viewRecord.do?id=1985>.

4. Recommended Additional Reading:

National Academy of Sciences, “The Impacts of Natural Disasters: A Framework for Loss Estimation,” 1999. http://www.nap.edu/openbook.php?record_id=6425.

ASIS International, “Organizational Resilience: Security, Preparedness, and Continuity Management Systems — Requirements with Guidance for Use,” ASIS SPC.1-2009;
<http://www.asisonline.org/guidelines/or.xml>.

LESSON 8 TOPIC: RISK AGGREGATION AND ANALYSIS

1. Lesson Goals/Objectives:

- Understand the principles of logical, qualitative, and quantitative integration of risk factors to establish an analytic conclusion
- Understand how to define risk by designated levels or relative comparison
- Become familiar with common ways of displaying the results of a risk assessment
- Understand the limits of the range of security risk approaches and models
- Understand sensitivity analysis and its use in assessing a risk model and the conclusions of a risk analysis

2. Discussion Topics:

- Compare and contrast the benefits and drawbacks of risk visualizations such as temperature charts, stop-light charts, likelihood and consequence graphs, risk curves, and whisker charts
- When is a simpler graphic warranted? When is a complex graphic better?
- When is it appropriate to compare risks solely within one sector or locality? When is it better to widen the comparison?
- How might statements from a risk assessment become misunderstood? What is the role of context in an assessment?
- Are there limits to the type of risks that should be displayed on one graphic?
- How might the results of a sensitivity analysis affect the degree of confidence the decision-maker should have in a model's results?
- How might an analyst account for the added risk caused by an infrastructure sector, or by components within a sector, that cause cascading effects within or across other sectors?

3. Required Reading:

SRMBOK, Chapter 6: Strategic Knowledge Areas.

National Research Council, Committee on Risk Characterization, *Understanding Risk: Informing Decisions in a Democratic Society*, P. C. Stern and H. V. Fineberg (eds.), Chapter 5: Integrating Analysis and Deliberation, Washington, D.C.: National Academy Press, 1996. <http://books.nap.edu/openbook.php?isbn=030905396X>.

Daniel Benjamin, "What Statistics Don't Tell Us," 2008.
http://www.brookings.edu/opinions/2008/0530_terrorism_benjamin.aspx.

Louis Anthony (Tony) Cox, Jr., "Some limitations of "Risk = Threat × Vulnerability × Consequence" for Risk Analysis of Terrorist Attacks," *Risk Analysis*, 28 (6), 2008, 1749-1761.

Louis Anthony (Tony) Cox, Jr., "What's Wrong with Risk Matrices?" *Risk Analysis*, 28 (2), 2008, 497-512.
http://www.evira.fi/attachments/english/research_on_animal_diseases_and_food/risk_assessment/riskmatrices.pdf.

LESSON 9 TOPIC: RISK COMMUNICATION

1. Lesson Goals/Objectives:

- Understand how to identify stakeholders and incorporate them into the risk analysis and risk management process
- Understand how to identify organizational dependencies in risk analysis and risk management
- Become familiar with organizations and partnerships that are used to promote international critical infrastructure protection cooperation and collaboration
- Understand how to communicate the context in which a risk analysis was performed as well as the uncertainties and other caveats associated with the results

2. Discussion Topics:

- Who “owns” risk associated with critical infrastructure nationally, regionally, or locally?
- Who “owns” the cyber problem in government and the private sector? How does each party communicate and coordinate with the other to jointly address cyber risk and supervisory control and data acquisition (SCADA) vulnerabilities?
- What are the key roles and responsibilities of the following with respect to critical infrastructure: Federal, State, and local governments; industry; academia; research and development (R&D) entities; and nongovernmental organizations?
- When should organizations that are needed to provide information for a risk assessment be engaged?
- When should the people who will be affected be engaged in the risk assessment?
- How might it be possible to identify a decision-maker’s willingness to accept risk?
- How might it be possible to identify the public’s willingness to accept risk?
- What are the costs and benefits of sharing uncertain information on terrorist threats?
- What are the strengths and weaknesses of simple and complex models for risk communication?
- What issues contribute to uncertainty? How much uncertainty undermines the validity of conclusions and recommendations?
- How do the various government and private entities with critical infrastructure responsibilities at different levels interact and collaborate with one another?
- What does the NIPP have to say regarding the international dimension of critical infrastructure?

3. Required Reading:

National Research Council, Committee on Risk Characterization, *Understanding Risk: Informing Decisions in a Democratic Society*, P. C. Stern and H. V. Fineberg (eds.), Chapter 6: Implementing the New Approach, Washington, D.C.: National Academy Press, 1996. <http://books.nap.edu/openbook.php?isbn=030905396X>.

Paul Slovic, "Perception of Risk," *Science*, 236 (4799), April 17, 1987, 280–285.

Paul Slovic, "Trust, Emotion, Sex, Politics, and Science: Surveying the Risk-Assessment Battlefield," *Risk Analysis*, 19(4), 1999, 689–701.

4. Recommended Additional Reading:

National Research Council, Committee on Risk Perception and Communication, "Improving Risk Communication," Executive Summary, 1989.

<http://www.nap.edu/catalog/1189.html>.

LESSON 10 TOPIC: ETHICS AND RISK MANAGEMENT

1. Lesson Goals/Objectives:

- Understand the principles of ethics involved in the risk assessment and management processes
- Understand the ethical challenges that may occur in data collection, modeling, analysis, and presentation of risk analysis

2. Discussion Topics:

- What are some potential pressures that might lead to a desire to skew risk results?
- What does sensitivity analysis reveal about a risk model? How should a decision-maker review the results of sensitivity analysis?
- How might the selection of experts for elicitation skew the results of an analysis? What are some steps that might prevent that from happening?
- How might the selection of variables, collection strategies, response formats, and scales skew the results of an analysis? What are some steps that might prevent that from happening?
- How can a risk assessment be “auditable”? What responsibility does an analyst have to enable an audit?
- What are the challenges in identifying “acceptable” risk?
- What are the potential liabilities and implications of having written risk reports? How should this affect organizational willingness to conduct a risk assessment?
- How would a “security or preparedness standard” help/hinder business transactions?

3. Required Reading:

National Research Council, Committee on Risk Characterization, *Understanding Risk: Informing Decisions in a Democratic Society*, P. C. Stern and H. V. Fineberg (eds.), Chapter 7: Principles of Risk Characterization, Washington, D.C.: National Academy Press, 1996. <http://books.nap.edu/openbook.php?isbn=030905396X>.

Security Analysis and Risk Management Association, “Code of Professional Ethics and Conduct,” <http://sarma.org/about/policies/codeofethics/>.

Stephen L. Derby and Ralph L. Keeney, “Risk Analysis: Understanding ‘How Safe is Safe Enough?’” *Risk Analysis* 1(3) 1981, 217–224.
[http://www.esm.ucsb.edu/academics/courses/286/Readings/Understanding%20How%20afe%20is%20Safe%20Enough.pdf](http://www.esm.ucsb.edu/academics/courses/286/Readings/Understanding%20How%20safe%20is%20Safe%20Enough.pdf).

LESSON 11 TOPIC: RISK MANAGEMENT

1. Lesson Goals/Objectives:

- Identify the opportunities to mitigate risk across the continuum of security risk
- Understand ways in which security investments reduce risk and methods of taking those reductions into account
- Understand the principles of cost–benefit analysis and the limitations in most security risk applications
- Become familiar with ways of considering risk reductions in one scenario as opposed to many
- Understand appropriate approaches to establishing metrics for risk management
- Understand how to use the results of risk analysis to make investment decisions in security and resiliency measures
- Discuss the relationship of security risk to safety, engineering, and other types of risk management and how these can be integrated in enterprise risk management

2. Discussion Topics:

- Identify a small number of potential security investments. When do the costs of those investments take place over their lifetime? When do the benefits begin to have effect? When do the benefits weaken, if at all?
- What would be the results of an effective security investment? How would you measure that? How would you defend further investments, if warranted?
- How does the perception of readiness or capabilities change as you move among the local, State, and Federal levels of government?
- What role should the public play in risk management?
- What role does a risk communication strategy play in risk management?

3. Required Reading:

SRMBOK, Chapter 8: Activity Areas; Chapter 9: Security Risk Management Enablers.

U.S. Government Accountability Office, “Natural Hazard Mitigation, Various Mitigation Efforts Exist, but Federal Efforts Do Not Provide a Comprehensive Strategic Framework,” GAO-07-403, 2007. <http://www.gao.gov/new.items/d07403.pdf>.

4. Recommended Additional Reading:

U.S. Federal Emergency Management Association, “Using HAZUS-MH for Risk Assessment How-To Guide,” FEMA 433, Step 5: Consider Mitigation Options, 2004. <http://www.fema.gov/library/viewRecord.do?id=1985>.

Robert T. Stafford Disaster Relief and Emergency Assistance Act (Public Law 93-288) as amended <http://www.fema.gov/about/stafact.shtm>.

National Fire Protection Association, “NFPA 1600: Standard on Disaster/Emergency Management and Business Continuity Programs,” 2010 Edition. <http://www.nfpa.org/assets/files/PDF/NFPA16002010.pdf>.

National Infrastructure Advisory Council, “A Framework for Establishing Critical Infrastructure Resilience Goals,” 2010. <http://www.dhs.gov/xlibrary/assets/niac/niac-a-framework-for-establishing-critical-infrastructure-resilience-goals-2010-10-19.pdf>.

LESSON 12 TOPIC: SECURITY RISK AND CRITICAL INFRASTRUCTURE DECISION SUPPORT

1. Lesson Goals/Objectives:

- Identify the types of decisions that security risk may inform (allocation of a security budget to a set of protective measures, capability investment, policy, access control procedures, exercise selection and design, continuity planning, analysis of alternatives, budget needs, etc.)
- Understand the characteristics of a risk model, methodology, and assessment that make it a good fit for a decision (i.e., degree they fit with the problem, stakeholders, and available data)
- Understand how security risk analysis can support Federal, State, local, tribal and territorial government decisions concerning the establishment or budgeting for critical infrastructure protection or resiliency programs
- Become familiar with common problems that cause risk assessments to fail to meet decision-makers' needs (e.g., poor design, poor scenario generation, and lack of feedback opportunities)
- Understand the factors that may influence a critical infrastructure decision in addition to security risk (e.g., urgency, public perception, precedent, potential for long-term success, etc.)

2. Discussion Topics:

- What might cause a political leader to choose a small and relatively unimportant project as the first part of a program to reduce critical infrastructure risk?
- What are some factors that complicate long-term risk-reduction investments?
- If a security risk is classified, how might that influence the decision-making process it is meant to support at Federal, State, and local levels of government?
- If you were making a resource allocation decision for anti-terrorism, what characteristics would you look for in a risk assessment?
- Compare and contrast the benefits and drawbacks of bottom-up and top-down planning at the state or regional level

3. Required Reading:

SRMBOK, Chapter 3: Security Governance; Chapter 11: Security Risk Management Integration.

Robin Gregory and Ralph L. Keeney, "Creating Policy Alternatives Using Stakeholder Values," *Management Science*, 40(8), 1994, 1035–1048.

4. Recommended Additional Reading:

National Research Council, "Review of the Department of Homeland Security's Approach to Risk Analysis," Washington, D.C.: The National Academies Press, 2010. http://www.nap.edu/catalog.php?record_id=12972.

LESSON 13 TOPIC: PRESENTATIONS

1. Lesson Goals/Objectives:

- Provide a critical analysis of a key critical infrastructure protection issue or critical infrastructure protection–related plan or policy and provide recommendations for improvement

2. Discussion Topics:

- Presentations

3. Required Reading:

- As required for research papers and presentations
-

LESSON 14 TOPIC: PRESENTATIONS

1. Lesson Goals/Objectives:

- Provide a critical analysis of a key critical infrastructure protection issue or critical infrastructure protection–related plan or policy and provide recommendations for improvement

2. Discussion Topics:

- Presentations

3. Required Reading:

- As required for research papers and presentations
-

LESSON 15 TOPIC: SUMMARY AND DISCUSSION OF CHOSEN TOPICS

1. Discussion Topics:

- Summary and discussion of lessons learned and observations from presentations in classes 13 and 14
- International aspects and perspectives on security risk management
- Current issues in risk management – what is needed to advance the discipline and use of risk management in critical infrastructure protection?
- What is the state of standards and guidelines in risk management and what is their impact on critical infrastructure protection?
- What professional associations and educational resources are at your disposal?
- Future directions in risk management. What remains to be done to make critical infrastructure protection risk management widely understood and better utilized?