**Certificate Program in Critical Infrastructure Security and Resilience**

**Course Number: XXXX**

**Assessing and Managing Risk to Critical Infrastructure Systems**

**University of XXXXXXX**

**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 an all-hazards risk assessment and management in the context of critical infrastructure security and resilience. It explores the strategic and operational context provided in the National Infrastructure Protection Plan (NIPP) and presents the challenges associated with understanding and taking action — including investment strategies— to manage risk within and across our diverse critical infrastructure sectors and composite systems. The course promotes subject-matter understanding, critical discussion of analytic approaches, and proficiency in communicating information on risk methodologies and their utilization in oral and written form. It also addresses the linkages to other critical infrastructure security and resilience competency areas — including government–private partnerships, information sharing, performance metrics, and decision support — as they relate to risk assessment and management. The development of required skills and knowledge will be promoted through readings, lectures, and in-class discussions, as well as practically exercised through written projects and in-class presentations.

Risk management is both a foundational concept and an analytic discipline deeply ingrained in the practical application of critical infrastructure security and resilience. It applies directly, albeit in different ways, to all of the critical infrastructure sectors and their composite systems as identified under the NIPP construct. Conceptually, its application in this mission area should be rather simple — by understanding the various risks to our critical infrastructure, we should be able to enhance their protection from and resilience to harmful events. However, to manage risks effectively, one must first be able to measure risks in a comprehensive way. This is where the simplicity of the concept of *risk management* and the complexity of *risk assessment* diverge. The underlying discipline of rigorous qualitative and quantitative assessment of all-hazards risks to our critical infrastructure is a relatively new phenomenon, 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 this debate.

Lastly, it is important to note that this course will address the complexities of critical infrastructure security and resilience from a “system-of-systems” perspective. Building upon the baseline characterization of our critical infrastructure and their associated dependencies/interdependencies provided in the introductory course, this course will explore the notion of a system and apply it to better understand how our critical infrastructure function and how they can fail or perform less than optimally under stress. This systems perspective will underpin the risk assessment and management framework which forms the focus of this course. The course will provide the learner with tools and techniques for describing systems in terms of internal components and dependencies with other systems, studying systems, and uncovering and managing risks affecting systems. While this course is technical in some aspects, it is geared toward learners without a background in the hard sciences or engineering. Mathematical concepts will be presented to the extent needed to apply the techniques introduced in class.

**credits conferred:** 3

**prerequisite:** Introduction to Critical Infrastructure Security and Resilience

The quantitative aspects of many forms of systems and risk analysis, particularly those involving mathematical expressions, probability, and statistical concepts, will be conveyed through assigned readings, discussed fully in class, and reflected in learner projects. While this course does not focus on the development of technical methodologies and advanced mathematical expressions for systems or risk analysis, learners will be able to understand and articulate those methodologies and mathematical expressions most commonly used to examine systems and quantify risk to them. Learners are advised to review basic algebra, probability, and statistics prior to the course if, in their own judgment, such review is needed.

**learner outcomes/objectives (as mapped against u.s. department of homeland security (dhs) critical infrastructure Security and resilience core competencies):**

Risk assessment and management activities support, and are supported by, the majority of the core competencies typically associated with the critical infrastructure security and resilience mission area. For example, when employed properly, risk assessment supports executive and managerial decision-making and justifies the development and prioritization of programs and investments designed to manage risk. Risk assessment also helps shape the development and employment of qualitative and quantitative metrics designed to measure the effectiveness and efficiency of risk management strategies and supporting programs and initiatives. Finally, risk assessment and management provide the common framework and lexicon for thinking and communicating about common challenges across the government-private partnership enterprise championed in the NIPP. This communication architecture enables effective multi-path information sharing and collaboration about risks between Federal, State, local, tribal, and territorial (FSLTT) government officials, and private sector infrastructure owners and operators.

This course is designed to enable learners to gain an understanding of the common critical infrastructure risk lexicon as well as to comprehensively explore the following focus areas:

**1. Risk Assessment:**

* Balancing the benefits, costs, decision support requirements, and practical implications associated with various risk assessment models and tools
* Selecting the risk assessment techniques and models best suited to the various types of critical infrastructure assets, systems, networks, and their interdependent connections
* Applying threat, vulnerability, and consequence assessment information and statistical data (when available) to calculate quantitative risk levels
* Evaluating the various attributes used to define risk assessment as related to all-hazards risks vs. risk assessment as applied in other areas (insurance, finance, engineering, etc.)

**2. Risk Mitigation Strategies:**

* Recognizing the complementary nature of prevention, protection, and resilience as methods of managing risks in interdependent critical infrastructure
* Performing risk assessments to inform the adoption of measures to address the physical, cyber, and human elements of critical infrastructure risk

**3. Systems Analysis**

* Explaininghow systems analysis fits within a risk management framework
* Deconstructingan infrastructure system into it basic elements with a focus on analyzing the function performed by the system, how it operates, and all relevant dependencies/ interdependencies
* Applying variousstructured analytic techniques to understand and assess the performance of infrastructure systems

**4. Partnership Building and Networking:**

* Recognizing risk management as a collaborative endeavor between critical infrastructure partners and the importance of stakeholder participation, including risk analyst – threat analyst collaboration
* Internalizing and applying a common risk lexicon to enable common understanding

**5. Information Collection and Reporting (Information Sharing):**

* Explaining how the intelligence analysis cycle functions as it relates to critical infrastructure security and resilience
* Recognizing intelligence reporting and threat data as a component of risk assessment and management
* Collecting qualitative and quantitative data on threats, vulnerabilities, and consequences for natural and man-made hazards
* Implementing the information collection process to support risk assessment and management

**6. Program Management:**

* Managing, timing, and scoping of risk assessment as management tasks
* Recognizing management factors, such as time, data collection, availability, and cost
* Identifying analytical risks (incorrect data, overconfidence, “paralysis by analysis,” uncertainty, and complexity)
* Establishing the definition of an “acceptable level of risk”

**7. Metrics and Program Evaluation:**

* Evaluating the effectiveness and efficiency of risk management programs and activities
* Applying performance measurement feedback to improve risk assessment and management processes and programs

**8. Sector-Specific Technical and Operational Expertise:**

Evaluating risks to physical assets and systems compared to logical assets, networks, and intangible assets

* Explaining dependencies and interdependencies and supply chain risk

**delivery method/course requirements:**

This course features a mix of theory and its practical applications to real-world infrastructure systems and their internal and external environments. Learners will develop an understanding of the subject-matter of the course and meet course objectives through a combination of assigned readings, lectures, group discussion, in-class exercises, written projects, and an in-class oral presentation. Learning will include a mix of independent study and group discussion and collaboration.

The assigned course readings include a variety of resources, such as government documents (legislation, executive orders, policies, plans, and strategies), academic readings (journal articles, research studies and reports), and third-party reviews (U.S. Government Accountability Office (GAO) reports, Congressional Research Service (CRS) reports, 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, particularly the external reviews, and from multiple perspectives. The instructor will facilitate the discussion by asking different levels of questioning (factual, analytical, and application of the material) to evaluate the depth of the learner’s comprehension of the content.

**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 the learner to keep up with the readings and participate in classroom discussions.
4. All cell phones and other electronic devices should be turned off before class begins.

**grading**

Class Participation 30%

Written project 30%

Project oral presentation 10%

Risk methodology critique point paper 30%

**written projects and presentations:**

1. **Written Project/Oral Presentation (40%):**

**Option 1**: The learner will prepare an 18-20 page (double-spaced) research paper on a relevant topic of interest in the area of risk assessment and management as applied to the critical infrastructure security and resilience mission area. The paper should clearly state a hypothesis and propose a solution to a known issue or problem. The paper should strive to support the hypothesis or solution recommended with authoritative reports, articles, interviews, or other data. The paper should be organized using the following format: problem statement, background (include key players, authorities, resources, etc.), discussion (presentation of the issue and alternative solutions, identifying pros and cons for each alternative), and recommendations (including rationale behind their selection). Footnotes and citations should be included on a separate sheet of paper in the proper format for review. The paper should focus on the benefits, drawbacks, and obstacles to the practical application of the proposed solution. The recommendations section should clearly describe the rationale for the solution of choice.

**Option 2**: In lieu of the above, learners may elect to develop an 18-20 page comprehensive written risk assessment and risk management strategy for a particular infrastructure system(s) utilizing one or a combination of the risk methodologies studied in the course. As a first step, learners will provide a detailed analysis of the infrastructure system itself, consisting of the following elements: system definition/description; summary of stakeholders and their perspectives on the system; block diagram of the system and description of all constituent elements; pertinent historical incidents affecting similar systems; and relationships with other systems, inputs, outputs, state variables, and strategies for monitoring performance. Next, learners will use their knowledge of the infrastructure system selected to comprehensively identify vulnerabilities, describe the types of threats that could exploit these vulnerabilities, and estimate how compromising the system will adversely affect the interests of one or more stakeholders. Learners will then identify various approaches/options for mitigating system vulnerabilities and evaluate them in terms of their costs and benefits and ability to reduce or manage risk. Finally, learners will define a set of performance metrics that can be used to measure the effectiveness and efficiency of the risk management approaches selected over time.

The research paper/written risk assessment and management strategy is due at the beginning of class in **Lesson 15**. Prior instructor approval of the topic for either of the two written project options is required. Learners must submit a one-paragraph written description of their proposed topic to the instructor for approval no later than the beginning of class in **Lesson 4**. All data used for this assignment will be properly cited; when data is unavailable, all assumptions with justification will be appropriately articulated.

Each learner will present his/her research topic (no more than 15-20 minutes in length) to the class during **Lessons 14-15**. Following each presentation, learners will have 5 additional minutes allotted to field questions from fellow learners. The presentation format will mirror that of the written project as detailed above.

1. **Risk Methodology Critique Point Paper (30%):**

Each learner will be expected to develop a 4-6 page point paper that provides a critical analysis of an existing risk assessment/management methodology, highlighting its relevance and ease of application to the critical infrastructure security and resilience mission area. Learners should review SARMApedia at <http://sarma-wiki.org/index.php?title=Category:Methodologies> for a listing of commonly used risk methodologies. Additional research and documentation will be required.

The learner’s analysis should address the following factors:

* Methodology’s origin, intended purpose, intended audience, and relation to a decision support process
* Description of the methodology’s major elements and attributes
* Characterization of the methodology’s quantification schema (or lack thereof)
* Approach to aggregating consequence, threat, and vulnerability into “risk” calculus
* Treatment of man-made and natural hazards
* Treatment of risk at sector and geographic levels
* Strengths of the approach
* Weaknesses of the approach
* Recommendations for methodology improvement

The instructor reserves the right to prevent multiple learners from studying the same methodology. Therefore, learners are required to submit their proposed methodology for study and at least one alternate choice to the instructor by the beginning of class in **Lesson 6**. Learner Risk Methodology Critiques are due at the beginning of class in **Lesson 11**. All data used for this assignment will be properly cited; when data is unavailable, all assumptions with justification will be appropriately articulated.

**expectations for classroom participation (30%):**

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

**incorporation of feedback**:

Multiple opportunities for constructive feedback between the instructor and learners will be provided over the period of the course. These feedback channels may take the form of group sessions or one-on-one sessions with the instructor. Learners will be afforded the opportunity to provide written mid-term feedback at the end of class on Lesson 6 and at the end of the course. On-line feedback to the instructor is also encouraged at any time throughout the course. Finally, the instructor will provide written feedback to the students on all oral and written assignments that form part of this course. Ongoing student dialogue with the instructor regarding research paper development, oral presentation preparation, and other in-class assignments is highly encouraged.

**course textbooks:**

The following are the primary textbooks for this course. These textbooks will be supplemented by additional readings accessible on-line, with website addresses provided in the lesson description section that follows.

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

Haimes, Yacov Y. *Risk Modeling, Assessment and Management*. 3rd ed. Hoboken, NJ: John Wiley & Sons, Inc., 2009.

Klir, George J. *Facets of Systems Science*. 2nd ed. New York: Springer, 2001.

**grading scale: school policy dependent**

**course outline**

**lesson 1 topic: course overview: risk as an analytic discipline**

**1. Lesson Goals/Objectives:**

* Discuss course scope, administrative requirements, instructional methodology, evaluation criteria, and feedback processes.
* Identify and apply the nine fundamental questions of risk management as related to risk assessment, communication, and mitigation.
* Identify the various types of risk as they pertain to the critical infrastructure and resilience mission area.
* Internalize the basic lexicon of systems analysis and risk assessment/management.
* Identify the composite elements of critical infrastructure risk (threat, vulnerability, and consequence).
* Examine the continuum of risk management, including prevention, protection, response, and recovery.
* Explain the levels at which systems and risk analysis are used in the critical infrastructure security and resilience mission area (policy, strategic, operational, tactical, etc.).

**2. Discussion Topics:**

* What is an infrastructure system? What is risk? What are the differences between systems analysis and risk analysis?
* What types of analysis are required to answer each of the nine fundament questions of risk?
* What makes infrastructure critical? What are the constituent elements of risk?
* What are the typical threat, vulnerability, and consequence elements associated with accidental infrastructure disruptions, terrorist attacks and natural hazard scenarios? How are they similar? How are they different?
* What decisions and/or resource investments might a critical infrastructure-focused risk assessment likely support?
* What is meant by the term “acceptable risk?” How does the acceptance of risk differ among the various elements of the NIPP stakeholder community?
* How do the requirements associated with the risk assessment process vary among the various NIPP stakeholders and stakeholder groups?
* What are the benefits of using risk-based approaches in this mission area?
* What is the DHS Critical Infrastructure Risk Management Enhancement Initiative (CIRMEI)?
* How do the international, GAO, and NIPP and Integrated Risk Management Framework (IRMF) risk frameworks detailed in the course readings differ? Is there one that seems more effective than the others? If so, why?
* Which are the most prevalent risk methodologies in use today? How are they similar/different? Who uses them and for what purpose?

1. **Required Reading:**

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

Lochry, R.R., R. D. Hensley, P. Flammer, D. R. Smith, R. G. Head, E. M. Henry, W. R., Nelson Hodson III, E. B., G. G. Carson, and J. F. Guilmartin. *Final Report of the USAF Academy Risk Analysis Study Team*. United States Air Force Academy, AD-729-223, 1971. <http://www.dtic.mil/dtic/tr/fulltext/u2/729223.pdf>

Kaplan, Stanley and B. John Garrick. “On the Quantitative Definition of Risk.” *Risk Analysis* 1, no. 1 (1981): 11-27. <http://josiah.berkeley.edu/2007Fall/NE275/CourseReader/3.pdf>.

National Research Council, Committee on Risk Characterization. *Understanding Risk: Informing Decisions in a Democratic Society*. Edited by P. C. Stern and H. V. Fineberg . Washington, DC: National Academy Press, (1996), Chapter 1. <http://books.nap.edu/openbook.php?isbn=030905396X>.

Matschulat, J.O. “An Introduction to the Concept and Management of Risk.” In *National Security Issues in Science, Law and Technology*, edited by Thomas A. Johnson, 291-357. New York: CRC Press, 2005.. <http://www.crcnetbase.com/doi/abs/10.1201/9781420019087.ch10>

Haimes, Yacov. “Total Risk Management.” *Risk Analysis* 11, no. 2 (2006): 169-71. <http://onlinelibrary.wiley.com/doi/10.1111/j.1539-6924.1991.tb00589.x/abstract>

U.S. Department of Homeland Security. *National Infrastructure Protection Plan*. Washington, DC, 2013. See Executive Summary and chap. 3, “Critical Infrastructure Environment.”

<http://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508_0.pdf>. .

U.S. Department of Homeland Security. *Risk Management Fundamentals: Homeland Security Risk Management Doctrine*. Washington, DC, 2011. <http://www.dhs.gov/xlibrary/assets/rma-risk-management-fundamentals.pdf>

George Mason University, The Center for Infrastructure Protection and Homeland Security. *The CIP Report* 10, no. 5 (November 2011). <http://tuscany.gmu.edu/centers/cip/cip.gmu.edu/wp-content/uploads/2013/06/CIPHS_TheCIPReport_November2011_RiskManagement.pdf>.

**4. Additional Recommended Reading:**

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

U.S. Department of Homeland Security. *DHS Infrastructure Taxonomy*. Ver. 3. Washington, DC, 2008. <http://www.hsdl.org/?view&doc=133262&coll=limited>.

**lesson 2 topic: the fundamentals of systems analysis**

**1. Lesson Goals/Objectives:**

* Recognize and apply important terms related to the definition and function of a system, including but not limited to:
  + Elements;
  + Relations;
  + Inputs;
  + Outputs;
  + States;
  + Objectives;
  + Values;
  + Constraints;
  + Exogenous Variables;
  + Random Variables;
  + Reliability;
  + Vulnerability;
  + Nodes;
  + Success Scenario;
  + Clusters;
  + Dependency; and
  + Interdependency
* Evaluate a system in terms of its objectives, constraints, input/output/state variables, elements, key nodes, and relationships among its composite elements.
* Construct reliability block diagrams of simple systems and use them to identify potential vulnerabilities and single-point failures.
* Explain the relationship between systems analysis and risk analysis and management.

**2. Discussion Questions:**

* What is a system? What are the fundamental elements of a system? What do we mean by “key nodes” and “clusters?”
* Why is it important to understand critical infrastructure security and resilience from a systems perspective?
* What are the typical types of external variables that impact system performance and behavior?
* Why is it important to be able to describe a system in terms of its elements and relationships?
* Why is it important to discuss how systems work in terms of objectives, constraints, and variables?
* What role does “point of view” play in defining a system?
* What is the relationship between “objectives” and “point of view?”
* How does defining a “security context” help in establishing a system scope?
* What is the relationship between “exogenous variables” and infrastructure interdependencies?
* How does system definition affect the interpretation of the term “interdependency?”
* How can knowledge of the elements and relations be used to construct reliability block diagrams? How can reliability block diagrams support risk assessment?

**3. In-Class Activity: Systems Description Exercise**

Learners will break down into groups and be asked to describe a particular infrastructure system in terms of its objectives, constraints, input variables, state variables, and output variables. Learners will also articulate the success scenario for the system. Learners will identify all relevant parts of the system and describe how they are related to one another. Learners will then use these descriptions to construct a corresponding reliability block diagram. The goal of this exercise is to provide learners with hands-on experience describing real infrastructure systems and creating simplified models of how a particular system functions.

**4. Required Reading:**

Ramo, Simon and Robin K. St. Clair. *The Systems Approach: Fresh Solutions to Complex Problems Through Combining Science and Practical Common Sense*.Anaheim, CA: KNI, Inc., 1998. <http://www.incose.org/productspubs/doc/systemsapproach.pdf>.

Sonnenberg, Amnon, John M. Inadomi, and Peter Bauerfiend. “Reliability Block Diagrams to Model Disease Management.” *Medical Decision Making*19, no. 2 (1999): 180-185. <http://www.ncbi.nlm.nih.gov/pubmed/10231080>

G. J. Klir, *Facets of Systems Science*, Springer, (2001), Excerpts from pp. 3-87.

Kaplan, Stan, Yacov Y. Haimes, and B. John Garrick. “Fitting Hierarchical Holographic Modeling into the Theory of Scenario Structuring and the Resulting Refinement to the Quantitative Definition of Risk.” *Risk Analysis* 21, no. 5 (2001): 807-819. <http://lyle.smu.edu/emis/cmmi5/Ibarra/DeskTop/White_Papers/Risk_Analysis/Risk_HHM.pdf>

Haimes, Yacok Y. *Risk Modeling, Assessment and Management*. 3rd ed. Hoboken, NJ: John Wiley & Sons, Inc., 2009. Excerpts from pages 57-88; 90-183.

**lesson 3 topic: basic approaches and models**

**1. Lesson Goals/Objectives:**

* Identify the various categories of risk assessment models (conceptual, formal, and computational).
* Explain the basic approaches to risk assessment (qualitative, quantitative, and semi-quantitative).
* Compare and contrast nominal, ordinal, interval, and ratio scales and the differences between natural and constructed scales.
* Identify and apply the factors that influence the selection of risk assessment models (data availability, timeframe required for analytic results, needs of decision-maker, available resources, etc.).

**2. Discussion Topics:**

* Compare and contrast the basic approaches to risk assessment. What are the strengths and weaknesses of each?
* What are the advantages and disadvantages of qualitative, quantitative, and semi-quantitative risk assessment model?
* What makes a good ordinal scale? What are some common mistakes in constructing scales?
* How does the selection of scale affect the scope and functionality of the risk assessment?

**3. Required Reading:**

SRMBOK, Chapter 5: Practice Areas.

Pariseau, Richard and Ivar Oswalt. “Using Data Types and Scales for Analysis and Decision Making.” *Acquisition Review Quarterly* 1, no. 2 (Spring 1994): 145-59. <http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA296380>.

National Research Council, Committee on Risk Characterization. *Understanding Risk: Informing Decisions in a Democratic Society*. Edited by P. C. Stern and H. V. Fineberg . Washington, DC: National Academy Press, (1996). Ch. 2, Judgment in the Risk Decision Process.  <http://www.nap.edu/openbook.php?isbn=030905396X>.

U.S. General Accounting Office, GAO/NSIAD-98-74, Threat and Risk Assessments Can Help Prioritize and Target Program Investments (1998). <http://www.loyola.edu/departments/academics/political-science/strategic-intelligence/intel/nsiad98-89.pdf>.

U.S. Department of Defense. “Standard Practice for System Safety.” MIL-STD-882D (February 2000). <http://www.system-safety.org/Documents/MIL-STD-882D.pdf>

Epstein, Joshua M. “Why Model?” *Journal of Artificial Societies and Social Simulation* 11, no. 4 (July 2008): 12. <http://jasss.soc.surrey.ac.uk/11/4/12.html>

1. **Recommended Reading:**

MacKenzie, C. Ronald and Mary E. Charlson. “Standards for the Use of Ordinal Scales in Clinical Trials.” *British Medical Journal*, 292, no. 4 (January 1986): 40-43. <http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1338986/>

The New England Chapter of the System Safety Society *System Safety: A Science and Technology Primer*. 2002. <http://www.system-safety.org/resources/SS_primer_4_02.pdf>.

**lesson 4 topic: threat assessment**

**\*special activity: learners must submit a one-paragraph written description of their proposed end-of-course project topic (research paper or risk assessment and risk management strategy) to the instructor for approval no later than the beginning of class.**

**1. Lesson Goals/Objectives:**

* Analyze the threat element of risk in the context of critical infrastructure security and resilience.
* Explain the various types of threat assessments and the roles they play in supporting a variety of critical infrastructure security activities (e.g., strategic assessments, tactical assessments, indications and warning, detection, attack assessment, and damage assessment).
* Evaluate methods of qualitatively comparing and quantifying the threat element of risk (frequency of occurrence, probability of attack, strength of indicators, etc.).
* Describe alternative approaches to exploring threat, beyond history, precedent, and intelligence (e.g., red cell analysis, game theory, role playing, etc.).

**2. Discussion Topics:**

* How does the threat differ in relation to the various types of terrorist groups on the domestic and international scene? Compare international terrorist groups with environmental extremists and domestic terrorist groups. 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, yet potentially catastrophic hazard? On an unprecedented hazard?
* What are the differences between strategic threat and tactical threat considerations (e.g., historical crime data vice current string of robberies)? Which is of more value to the risk assessment process?
* How might threat analysis, especially the warning component, influence the bigger picture risk calculus?
* Compare the threat assessment for a given 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? What are other principal sources of threat information?
* What are the primary sources of data for naturally occurring threats and hazards? How does the natural hazard threat assessment process differ from that used to assess malicious actor threats?
* How would a strategic threat change into a tactical threat upon receipt of a credible threat 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*. Edited by P. C. Stern and H. V. Fineberg . Washington, DC: National Academy Press, (1996). Ch. 4, Analysis. <http://www.nap.edu/openbook.php?isbn=030905396X>.

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>.

George Mason University, Critical Infrastructure Protection Program. *Critical Infrastructure Protection: Elements of Risk*. (2007). Chapter 2 “Intelligence Analysis for Strategic Risk Assessments.” <http://cip.gmu.edu/wp-content/uploads/2014/03/ElementsofRiskMonograph.pdf>

Steinberg, Alan N. “An Approach to Threat Assessment.” In *Harbour Protection Through Data Fusion Technologies*, edited by Elisa Shahbazian, Galina Rogova, and Michael J. DeWeert, 95-108. Dordrecht, NL: Springer, 2005. <http://link.springer.com/chapter/10.1007%2F978-1-4020-8883-4_16?LI=true>

Homeland Security Institute. *Risk Analysis and Intelligence Communities Collaborative Framework*. (2009). <http://www.homelanddefense.org/downloads/Risk-Intel%20Collaboration%20Final%20Report.pdf>

**4. Recommended Additional Reading:**

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

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

Rosoff, H. and D. von Winterfeldt. “A Risk and Economic Analysis of Dirty Bomb Attacks on the Ports of Los Angeles and Long Beach.” *Risk Analysis* 27, no. 3(2007): 533-46. <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>.

**lesson 5 topic: system failure and vulnerability**

**\*special activity: learners are required to submit their proposed risk methodology for critique and at least one alternate choice to the instructor by the beginning of class.**

**1. Lesson Goals/Objectives:**

* Analyze the concepts associated with infrastructure system failure modes and effects analysis (FMEA) and anticipatory failure determination analysis (AFDA) and explore ways to tailor these analytic techniques to various infrastructure system types.
* Analyze vulnerability in the context of the critical infrastructure security and resilience risk assessment process.
* Explain methods of qualitatively comparing and quantifying vulnerability (probability, event trees, fault trees, minimal cut sets, checklists, and judgments).

**2. Discussion Topics:**

* What are the principal factors that cause infrastructure systems to fail or perform below standard?
* What is a FMEA? An AFDA? Is FMEA or AFDA the same as a vulnerability assessment? Why or why not?
* What kind of analysis is a prerequisite to performing a FMEA or an AFDA?
* How does a FMEA or an AFDA compare to risk assessment in general?
* How do the results of a FMEA or AFDA fit within the scope of systems analysis?
* In what ways can FMEA or AFDA be modified to support extended analysis of a system?
* What is meant by the term “vulnerability” in the context of critical infrastructure security and resilience?
* What do we mean by the ability to withstand an attack or an unacceptable degree or level of consequence? How might that consideration change the focus of a risk assessment?
* How do critical infrastructure dependencies and interdependencies complicate the vulnerability assessment process?
* How might co-location of various different assets or asset types 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 infrastructure sector? 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.

S. Kaplan, S. Visnepolschi, B. Zlotin, and A. Zusman, “New Tools for Failure and Risk Analysis: An Introduction to Anticipatory Failure Determination (AFD) and the Theory of Scenario Structuring,” Ideation International, (1999). <http://www.ideationtriz.com/new/materials/AFDNewToolsbook.pdf>

Reason, James. “Human Error: Models and Management.” *British Medical Journal* 380 (March 2000). <http://www.paediatricchairs.ca/safety_curriculum/domain5_docs/HumanErrorReason.pdf>

Haimes, Yacov Y. “On the Definition of Vulnerabilities in Measuring Risks to Infrastructures.” *Risk Analysis* 26, no. 2 (2006): 293–96. <http://onlinelibrary.wiley.com/doi/10.1111/j.1539-6924.2006.00755.x/abstract>

Paul W. Parfomak, Congr. Research Serv.*,* RL33206,Vulnerability of Concentrated Critical Infrastructure: Background and Policy Options (2008), <http://www.fas.org/sgp/crs/homesec/RL33206.pdf>.

French, Geoffrey S. 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/doi/pdf/10.1061/41170%28400%2995>.

American Society for Quality. “Failure Mode Effects Analysis (FMEA).” 2011. <http://asq.org/learn-about-quality/process-analysis-tools/overview/fmea.html>.

Resource Engineering Inc. “FMEA Pitfalls and Limitations.” 2011. <http://www.qualitytrainingportal.com/resources/fmea/fmea_pitfalls.htm>.

Ideation International Inc. “AFD (Anticipatory Failure Determination)” 2011. <http://www.ideationtriz.com/AFD.asp>.

**4. Recommended Additional Reading:**

McDermott, R. E., R. J. Mikulak, and M. R. Beauregard.

*The Basics of FMEA*. Quality Resources, 1996.

Cutter, S.L., Boruff, B.J., and Shirley, W.L. “Social Vulnerability to Environmental Hazards.” *Social Science Quarterly* 84, no. 2 (2003): 242–61. <http://www.colorado.edu/hazards/resources/socy4037/Cutter%20%20%20Social%20vulnerability%20to%20environmental%20hazards.pdf>.

McGill, William L., Bilal M. Ayyub, and Mark Kaminskiy. “Risk Analysis for Critical Asset Protection.” *Risk Analysis* 27, no. 5 (2007): 1265–81. <http://onlinelibrary.wiley.com/doi/10.1111/j.1539-6924.2007.00955.x/abstract>

U.S. Gov’t Accountability Office, GAO-09-851, Biosafety Laboratories: BSL-4 Laboratories Improved Perimeter Security Despite Limited Action by CDC, (2009). <http://www.gao.gov/new.items/d09851.pdf>.

**lesson 6 topic: likelihood estimation**

**1. Lesson Goals/Objectives:**

* Evaluate the interactions among the threat, vulnerability, and consequences variables of risk.
* Explain the various qualitative methods for integrating threat and vulnerability.
* Analyze conditional probabilities, possibility trees, event trees, and other approaches to probabilistic likelihood estimation.
* Execute event tree analysis to understand and describe how systems work and why they fail.
* Describe cascading effects in a Consequence Assessment.
* Analyze cases that present complex interactions among threat, vulnerability, and consequence variables (such as cascading effects, multi-staged attacks, biological events, and natural hazards with effects over time).

**2. Discussion Topics:**

* What is meant by the term “probablistic likelihood?” How is it quantified?
* 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*?
* What are the various qualitative methods for integrating threat and vulnerability? How do they differ? Are they “user friendly?”
* How do existing risk models/methodologies quantify and combine the threat and vulnerability elements of risk?
* What are the major features of the conditional probabilities, event tree, and other approaches to probabilistic likelihood estimation? Advantages/disadvantages of each? Is one approach better or easier to use than the rest?
* What is the purpose of an event tree? How are event trees the same or different than possibility trees? What is the difference between an event tree and a timeline?
* What role does conditional logic play in event tree/possibility tree analysis?
* What are some potential pitfalls associated with performing an event tree analysis? What are strengths of the method? Weaknesses?
* What are some real-world examples that represent complex interactions among the threat, vulnerability, and consequence element of risk (such as cascading effects, multi-staged attacks, biological events, and natural hazards with effects over time)?
* How is likelihood determined in the context of a cyber-attack or non-malicious outage?
* How do infrastructure dependencies affect risk management considerations/options? How does social vulnerability affect risk management considerations/options?

**3. In-Class Activity: Event Tree Analysis Exercise:**

Learners will break into groups and be asked to construct an event tree that traces out all possible ways that a particular infrastructure system might fail following exposure to some specified hazardous situation (e.g., explosion, earthquake, pipe failure, etc.). The goal of this assignment is to provide learners with practice working with mutually exclusive, collectively exhaustive possibilities of what can occur at different points along a timeline of infrastructure system performance.

**4. Required Reading:**

Pate-Cornell, M. E. “Fault Trees vs. Event Trees in Reliability Analysis.” *Risk Analysis* 4, no. 3 (1984): 177-86. <http://onlinelibrary.wiley.com/doi/10.1111/j.1539-6924.1984.tb00137.x/abstract>

Rinaldi, Steven M., James P. Peerenboom, and Terrence K. Kelly. “Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies” *IEEE Control Systems Magazine* (December 2001): 11-25. <http://www.ce.cmu.edu/~hsm/im2004/readings/CII-Rinaldi.pdf>.

Newhall, C.G. and R. P. Hoblitt. “Constructing Event Trees for Volcanic Crises.”

*Bulletin of Volcanology* 64, no.1 (March 2002): 3-20.

<http://link.springer.com/article/10.1007%2Fs004450100173>.

Rausand, Marvin. “Chapter 3: System Analysis: Fault Tree Analysis” *System Reliability Theory*. 2nd ed. Wiley, 2004. <http://frigg.ivt.ntnu.no/ross/slides/fta.pdf>

Little, Eric G. and Galina L. Rogova. “An Ontological Analysis of Threat and Vulnerability.” in *Proceedings of the FUSION 2006-9th International Conference on Multisource Information Fusion*. Florence, Italy, July 10-13 2006. <http://www.researchgate.net/publication/228625858_An_ontological_analysis_of_threat_and_vulnerability>

George Mason University, The Center for Infrastructure Protection and Homeland Security. *The CIP Report* 10, no. 2 (August 2011).

<http://tuscany.gmu.edu/centers/cip/cip.gmu.edu/wp-content/uploads/2013/06/CIPHS_TheCIPReport_August2011_Interdependencies.pdf>. **lesson 7 topic: consequence assessment**

**1. Lesson Goals/Objectives:**

* Analyze consequence in the context of critical infrastructure security and resilience risk assessment.
* Explain how consequence units of measurement and valuation scales are determined and how they interact.
* Analyze the differences between direct and indirect consequences in the context of critical infrastructure risk.
* Apply the Weighted Ranking Method (WRM) and Analytic Hierarchy Process (AHP) to estimate the level of concern or impact that would be associated with a variety of disruptive situations.

**2. Discussion Topics:**

* What are the various categories of critical infrastructure–related consequences? Is there a relative priority among them?
* What are the various methods used to assess potential consequences in the context of critical infrastructure risk, including quantification of the consequence element of risk?
* What are the various sources of data and other information used to support consequence assessment?
* Why are there different values for a statistical life?
* What are the differences between direct and indirect consequences in the context of critical infrastructure risk?
* 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 fatalities? Why would a model include estimates of the number of “worried well?”
* How do willingness-to-pay models, value of a statistical life, and other methods of assigning monetary values relate to the consequence element of infrastructure risk?
* What are the types of consequences and what is the extent of potential consequences that an attack on the cyber components of a critical infrastructure asset or system might have?
* How do the WRM and AHP compare? What are the strengths, weaknesses, and limitations of each?
* What role does Pairwise Ranking play in estimating the potential impact of system incidents?

**3. Required Reading:**

Fischhoff, Baruch, Stephen R. Watson, and Chris Hope. “Defining Risk.” *Policy Sciences* 17 (1984): 123-39, <http://link.springer.com/article/10.1007%2FBF00146924?LI=true>.

Jones, Morgan D. *The Thinker’s Toolkit: 14 Powerful Techniques for Problem Solving*. Crown Business, 1998. 246-81.

National Research Council. *The Impacts of Natural Disasters: A Framework for Loss Estimation*. Washington, DC: The National Academies Press, 1999. <http://www.nap.edu/openbook.php?record_id=6425>.

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

Saaty, T. L. “Decision Making with the Analytic Hierarchy Process.”

*International Journal of Services Sciences* 1, no. 1 (2008): 83-98. <http://www.colorado.edu/geography/leyk/geog_5113/readings/saaty_2008.pdf>.

Concordia University. “Pairwise Ranking.” *Coast Guard Process Improvement Guide* (2011): 26-27. <http://web2.concordia.ca/Quality/tools/18pairwise.pdf>.

**4. Recommended Additional Reading:**

ASIS International. *Organizational Resilience: Security, Preparedness, and Continuity Management Systems — Requirements with Guidance for Use*. ASIS, 2009. <https://www.asisonline.org/Standards-Guidelines/Standards/published/Pages/Organizational-Resilience-Security-Preparedness-and-Continuity-Management-Systems-Requirements-with-Guidance-for-Use.aspx?cart=2d698c9906f142c4800cd7522934ed02>.

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>.

**lesson 8 topic: all-hazards risk scenario generation**

**1. Lesson Goals/Objectives:**

* Describe how to set goals and objectives at the outset of a risk management project.
* Assess the operational context of the various critical infrastructure sectors and their composite assets, facilities, systems, networks, and interdependent connections.
* Identify methods for screening a set of critical infrastructure assets (physical, cyber, and human) for criticality, including multi-attribute utility theory.
* Analyze the role that scenario generation plays in enabling comparative risk assessment.
* Apply multiple methods of generating plausible threat and hazard scenarios and evaluate scenarios for completeness and appropriateness (including internal consistency and documentation of explicit assumptions and variables).

**2. Discussion Topics:**

* How does the interaction of the decision-maker, threat/hazard type, and the nature of the critical infrastructure of concern influence the context and parameters of a risk assessment?
* How do 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/asset types/systems? What are the major nuances?
* 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., policy, strategic, operational, tactical) influence the need for detail in a scenario?
* When is it appropriate to use a worst-case scenario? How do you define “worst-case”? How might you limit severity of a scenario to a reasonable extent without impacting the training value of an exercise or walkthrough of the threat event? What are the key factors you would consider in so doing?
* What is meant by the phrase “failure of imagination?” How does this phrase apply to systems analysis?
* To what extent does divergent-convergent thinking mitigate “failure of imagination?”
* What are the strengths, weaknesses, and limitations of divergent-convergent thinking? Is divergent-convergent thinking a suitable technique for use in systems analysis?

**3. In-Class Activity: Divergent-Convergent Thinking Exercise:**

In this exercise, learners will consider a particular system and will be asked to generate a representative list of plausible threats with the potential to compromise the system. Learners will work in groups and apply the Divergent-Convergent Technique to develop a list of scenarios. For each scenario, learners will employ their knowledge of the system to fully explain how the threat could cause harm.

**4. 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*. Edited by P. C. Stern and H. V. Fineberg . Washington, DC: National Academy Press, (1996). Chapter 3: Deliberation. <http://www.nap.edu/openbook.php?isbn=030905396X>.

Jones, Morgan D. *The Thinker’s Toolkit: 14 Powerful Techniques for Problem Solving*.

Crown Business, 1998: 80-86.

Morgan, M. Granger, H. Keith Florig, Michael L. DeKay, and Paul Fischbeck. “Categorizing Risks for Risk Ranking.” *Risk Analysis* 20, no. 1 (2000): 49-58. <http://onlinelibrary.wiley.com/doi/10.1111/0272-4332.00005/abstract>.

Haimes, Yacov Y., Stan Kaplan, and James H. Lambert. “Risk Filtering, Ranking, and Management Framework Using Hierarchical Holographic Modeling.”

*Risk Analysis* 22, no. 2 (2002): 383-97. <http://lyle.smu.edu/emis/cmmi5/Ibarra/DeskTop/White_Papers/Risk_Analysis/Risk_RFRM.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: A Letter Report. Washington, DC: The National Academies Press, 2007. <http://www.nap.edu/catalog.php?record_id=12073>.

Bitzer, Edward G. and Roger Johnston. “Creative Adversarial Vulnerability Assessments.” *Journal of Physical Security* 2, no. 1, paper 5 (2007).

<http://jps.anl.gov/vol.2/5-Creative_Assessments.pdf>.

**5. Recommended Additional Reading:**

Khan, Faisal. “Use Maximum-Credible Accident Scenarios for Realistic and Reliable Risk Assessment.” *Chemical Engineering Progress Magazine* (November 2001): 56-64. <http://people.clarkson.edu/~wwilcox/Design/riskasss.pdf>.

John Moteff, Claudia Copeland, & John Fischer, Cong. Research Serv., RL 31556, Critical Infrastructures: What Makes Infrastructure Critical? (2002). <http://www.libertysecurity.org/IMG/pdf/CRS_Report_-_What_makes_an_Infrastructure_Critical_-_30.08.2002.pdf>.

U.S. Federal Emergency Management Association, FEMA 433, Using HAZUS-MH for Risk Assessment How-To Guide, Step 1: Identify Hazards (2004), <http://www.fema.gov/library/viewRecord.do?id=1985>.

National Commission on Terrorist Attacks upon the United States. *The 9/11 Commission Report*. 2004. <http://www.9-11commission.gov/report/911Report.pdf>.

Matschulat, James O. “An Introduction to the Concept and Management of Risk,” in *National Security Issues in Science, Law and Technology*, edited by Thomas A. Johnson New York: CRC Press, 2005, 291-357. <http://www.crcnetbase.com/doi/abs/10.1201/9781420019087.ch10>.

van Notten, Philip. “Scenario Development: A Typology of Approaches,” in Think Scenarios, Rethink Education. OECD, 2006. <http://www.oecd.org/site/schoolingfortomorrowknowledgebase/futuresthinking/scenarios/scenariodevelopmentatypologyofapproaches.htm>.

**lesson 9 topic: risk aggregation, analysis, and ethics**

**1. Lesson Goals/Objectives:**

* Analyze the principles of logical, qualitative, and quantitative integration of risk factors to establish an analytic conclusion.
* Describe how to define risk by designated levels or relative comparison.
* Explain common ways of displaying the results of a risk assessment.
* Discuss the limits of the range of various risk approaches and models.
* Analyze sensitivity analysis and its use in assessing a risk model and the conclusions of a risk analysis.
* Discuss the ethical considerations associated with the risk assessment and management process.

**2. Discussion Topics:**

* What are 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?
* 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 associated with an infrastructure sector, or by components within a sector, that cause cascading effects within that sector or across other sectors?
* What does sensitivity analysis reveal about a risk model? How should a decision-maker review the results of sensitivity analysis?
* How might the process used to select experts for elicitation itself 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?

**3. Required Reading:**

SRMBOK. Chapter 6: Strategic Knowledge Areas.

Derby, Stephen L. and Ralph L. Keeney, “Risk Analysis: Understanding ‘How Safe is Safe Enough?’” *Risk Analysis* 1, no. 3 (1981): 217–224. <http://onlinelibrary.wiley.com/doi/10.1111/j.1539-6924.1981.tb01418.x/abstract>.

National Research Council, Committee on Risk Characterization. *Understanding Risk: Informing Decisions in a Democratic Society*. Edited by P. C. Stern and H. V. Fineberg . Washington, DC: National Academy Press, (1996). Chapter 5: Integrating Analysis and Deliberation and Chapter 7: Principles of Risk Characterization. <http://books.nap.edu/openbook.php?isbn=030905396X>.

Benjamin, Daniel. “What Statistics Don’t Tell Us.” *Brookings* (May 30, 2008). <http://www.brookings.edu/opinions/2008/0530_terrorism_benjamin.aspx>.

Cox, Jr., Louis Anthony (Tony). "Some Limitations of "Risk = Threat × Vulnerability × Consequence" for Risk Analysis of Terrorist Attacks." *Risk Analysis* 28, no. 6 (2008): 1749-61. <http://onlinelibrary.wiley.com/doi/10.1111/j.1539-6924.2008.01142.x/abstract>

Cox, Jr., Louis Anthony (Tony). "What’s Wrong with Risk Matrices?" *Risk Analysis* 28, no. 2 (2008): 497-512. <http://onlinelibrary.wiley.com/doi/10.1111/j.1539-6924.2008.01030.x/abstract>

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

**lesson 10 topic: stakeholder engagement and risk communication**

**1. Lesson Goals/Objectives:**

* Identify the organizations and partnerships that are used to promote international critical infrastructure security and resilience risk management.
* Analyze the complexities of the NIPP Partnership Framework as it relates to the critical infrastructure security and resilience risk analysis/management process.
* Explain how to identify partner dependencies in risk analysis, management, and communication.
* Explain the role that an effective risk communication strategy plays in risk management.

**2. Discussion Topics:**

* Who “owns” risk associated with critical infrastructure nationally, regionally, or locally? In the cyber world?
* Do other members of the international community use a sector construct to help organize their approach to critical infrastructure risk analysis and management? How do the various international approaches differ from the U.S. construct? How does the international community view risk, especially with regards to their sectors or other constructs?
* What are the key roles and responsibilities of the following with respect to critical infrastructure risk assessment and management: FSLTT 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? How does this engagement take place? What are the barriers to effective collaboration in this area?
* What role does a risk communication strategy play in risk management?
* 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 risk assessment and management? Are there structures and processes in place to facilitate international risk management and address problems that cross international boundaries and borders?

**3. Required Reading:**

Slovic, Paul. "Perception of Risk." *Science* 236, no. 4799 (April 17, 1987): 280-85. <http://socsci2.ucsd.edu/~aronatas/project/academic/risk%20slovic.pdf>.

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

Slovic, Paul. "Trust, Emotion, Sex, Politics, and Science: Surveying the

Risk-Assessment Battlefield." *Risk Analysis* 19, no. 4 (1999): 689-701.

<http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CDoQFjAA&url=http%3A%2F%2Fciteseerx.ist.psu.edu%2Fviewdoc%2Fdownload%3Fdoi%3D10.1.1.118.417%26rep%3Drep1%26type%3Dpdf&ei=551QUeDUC8jD0QH7iIHICA&usg=AFQjCNHFKQlcpK1GvHScoECjT21bWLhbCw&sig2=jHcBEQvUq3nKqCbn5R6Szw&bvm=bv.44158598,d.dmQ&cad=rja>

U.S. Department of Homeland Security. *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*. Washington, DC, 2013, pp. 15-20, 23-25. <http://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508_0.pdf>.

Klaver, Marieke, Eric Luiijf, and Albert Nieuwenhuijs. *Good Practices Manual for CIP Policies: For Policy Makers in Europe*. (2011). <https://www.tno.nl/content.cfm?context=thema&content=inno_publicatie&laag1=893&laag2=910&laag3=1&item_id=836&Taal=2>.

U.S. Department of Homeland Security. “Partnerships.” *Critical Infrastructure Resource Center*. <http://training.fema.gov/EMIWeb/IS/IS860b/CIRC/NIPPinfo.htm#item2>.

**4. Recommended Additional Reading:**

National Research Council. "Summary." *Improving Risk Communication*. Washington, DC: The National Academies Press, 1989, 1-13. <http://www.nap.edu/catalog/1189.html>.

**lesson 11 topic: risk management approaches**

**\*special activity: learner risk methodology critiques are due at the beginning of class.**

**1. Lesson Goals/Objectives:**

* Identify and describe commonly used approaches to help mitigate risk to critical infrastructure systems across the continuum of all-hazards risk.
* Explain how to use the results of the risk assessment process to inform investments in security and resilience.
* Identify and describe approaches that are focused on scenario-based risk mitigation.
* Explain the relationship of critical infrastructure risk to safety, engineering, and other types of risk management and how they can be integrated in an enterprise risk management framework.
* Assess the Pros/Cons/Fixes technique and its application to the determination of alternative risk management strategies.

**2. Discussion Topics:**

* Identify the general range of risk mitigation strategies relevant to the critical infrastructure and resilience mission area. What are the costs and benefits of each? Are they mutually exclusive?
* When are the costs of those investments realized over their lifetime? When do the benefits begin to have effect? When do the benefits weaken, if at all?
* What are the criteria for an effective security or resilience investment? How would outcomes/performance be measured? How would you defend further investments, if warranted?
* How do the perception of risk and the risk mitigation calculus vary between the FSLTT levels of government? Between government and the private sector?
* What are the strengths of the Pros/Cons/Fixes method? What are its weaknesses? What types of information are needed to complete a Pros/Cons/Fixes analysis?
* How do the results of analysis methods such as FMEA, AFDA, fault tree analysis, and event tree analysis assist with identifying alternative protection strategies for a system?

**3. In-Class Activity: Risk Management Exercise**

In this exercise, learners will be asked to propose and describe various alternative approaches to effectively manage risk in the context of a particular infrastructure system using the Pros/Cons/Fixes method.

**4. Required Reading:**

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

Jones, Morgan D. *The Thinker’s Toolkit: 14 Powerful Techniques for Problem Solving*. Crown Business, (1998), 72-79.

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

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

Norman, Thomas L. *Risk Analysis and Security Countermeasure Selection*.

New York: CRC Press, 2009, 67-81.

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

**5. Recommended Additional Reading:**

Robert T. Stafford Disaster Relief and Emergency Assistance Act, Pub. L. No. 93-288, as amended. Available at <http://www.fema.gov/about/stafact.shtm>.

National Fire Protection Association. *NFPA 1600: Standard on Disaster/Emergency Management and Business Continuity Programs*. NFPA, 2013. <http://www.nfpa.org/codes-and-standards/document-information-pages?mode=code&code=1600>.

**lesson 12 topic: risk management decision support and performance measurement**

**1. Lesson Goals/Objectives:**

* Identify the types of decisions that the risk assessment and management process might inform (e.g., 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.).
* Identify the characteristics of a risk model, methodology, or assessment that make it a good decision enabler (i.e., degree they fit with the problem, stakeholders, and available data).
* Explain how the risk assessment and management process can support FSLTT government decisions concerning the establishment or budgeting for critical infrastructure security or resilience programs.
* Evaluate 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).
* Evaluate the factors that may influence decision-making outside the context of risk (e.g., urgency, public perception, precedent, potential for long-term success, etc.).
* Explain the ways in which the effectiveness and efficiency of critical infrastructure security and resilience strategies, plans, and programs may be measured over time.
* Identify and explain measurable indicators of systems performance as well as how system performance relates to risk.
* Use the Indicators and Signposts of Change methodology to track system performance over time.

**2. Discussion Topics:**

* What are the types of decisions that the risk assessment and management process risk might help to inform?
* How do critical infrastructure and resilience risk assessment/management processes and decision support processes intersect at various levels of government? Within the private sector? Between government and the private sector?
* What are some factors that complicate long-term risk-based planning and resource investments and performance measurement?
* If a security risk is classified, how might that influence the decision-making process it is meant to support at various levels of government?
* How are outcomes/performance related to critical infrastructure security and resilience measured at various levels of government and within the private sector? Are there commonly used metrics?
* Is there collaboration in performance measurement between the government and the private sector? If so, at what level(s)?
* What are the other factors that may “trump” the classical consideration of risk as discussed in this course in the mind of a decision-maker?
* What types of indicators would you look for to measure the performance of the electric power grid? Water distribution system? Mass transit system?
* How does system performance relate to risk?
* How can the Indicators and Signposts of Change methodology be used to inform decisions to issue warnings to decision-makers?

**3. In-Class Activity: Performance Measure Development Exercise**

In this exercise, learners will be asked to propose and describe metrics used for understanding and tracking the performance of a particular critical infrastructure system, subsystem, or asset over time. Afterwards, learners will develop a strategy for collecting data to assign values to these metrics and discuss data quality issues. The goal of this assignment is to provide learners with an experience in developing measures that can be used to evaluate the present condition of a system in terms of risk.

**4. Required Reading:**

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

Gregory, Robin and Ralph L. Keeney. “Creating Policy Alternatives Using Stakeholder Values.” *Management Science* 40, no. 8 (August 1994): 1035-48. <http://mansci.journal.informs.org/content/40/8/1035.abstract?ijkey=fc4834000d9cb28a0c37ce3211e6a3d90822d91f&keytype2=tf_ipsecsha>.

Central Intelligence Agency. *A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis*. (2009), <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/Tradecraft%20Primer-apr09.pdf>.

Hubbard, Douglas W. *How to Measure Anything: Finding the Value of Intangibles in Business*. 2nd ed. Hoboken, NJ: Wiley, 2010.

National Research Council. *Review of the Department of Homeland Security’s Approach to Risk Analysis*. Washington, DC: The National Academies Press, 2010. <http://www.nap.edu/openbook.php?record_id=12972>.

**5. Recommended Additional Reading:**

Betts, Richard K. “Analysis, War and Decision: Why Intelligence Failures are Inevitable.” *World Politics* 31, no. 1 (October 1978): 61-89. <http://journals.cambridge.org/action/displayAbstract?fromPage=online&aid=7629164&fileId=S0043887100010182>.

Clemen, Robert T. *Making Hard Decisions: An Introduction to Decision Analysis*. Cengage, 1997.

**lesson 13 topic: risk management as a dynamic, evolutionary concept**

**1. Lesson Goals/Objectives:**

* Apply future forecasting techniques to anticipate how different infrastructure systems and associated risks may evolve over time and why.
* Explain the importance of taking a forward-looking view regarding how infrastructure and systems in general, together with risk, evolve over time.
* Describe ways in which critical infrastructure risk management and performance measurement approaches might evolve over time.
* Explain how key critical infrastructure stakeholder relationships and dependencies and interdependencies considerations might evolve over time.

**2. Discussion Questions:**

* How do you expect the critical infrastructure operating environment to evolve over time?
* How do you expect critical infrastructure threats and vulnerabilities to evolve over time?
* What are some potentially significant drivers of such change?
* What is the difference between a prediction and an estimate in this calculus? Which are more useful? Which are easier to obtain?
* Is it important to study infrastructure evolution? Why?
* How does such study tie in with risk assessment and management in general?
* How will key critical infrastructure stakeholder relationships and dependencies and interdependencies considerations evolve over time?
* How will we best measure and manage critical infrastructure risk and measure performance in the future?

**3. In-Class Activity: Technology Forecasting Exercise**

In this exercise, learners will be assigned to examine a specific critical infrastructure sector or system and will be asked to apply one or more future forecasting techniques to explore alternative ways the sector/system and associated risks might evolve over time. Special attention will be paid to what new vulnerabilities might emerge over time, and what threats may rise to shape new risks. The goal of this exercise is not to come up with absolute predictions, but to describe the range of plausible futures and how they impact any assessment of risk.

**4. Required Reading:**

Gordon, Theodore Jay. *Cross-Impact Method*. United Nations, 1994. <http://www1.ximb.ac.in/users/fac/dpdash/dpdash.nsf/23e5e39594c064ee852564ae004fa010/2a7a6240bcf05ebde5256906000a7322/$FILE/Cross-im.pdf>.

Central Intelligence Agency. *A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis*. (2009). <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/Tradecraft%20Primer-apr09.pdf>.

National Research Council. *Avoiding Surprise in an Era of Global Technology Advances*.Washington, DC: National Academy Press, 2005. <http://www.nap.edu/openbook.php?isbn=0309096057>.

Toffler Associates. *Guarding Our Future: Protecting our Nation’s Infrastructure* Manchester, MA: Toffler Associates, 2008. <http://www.toffler.com/assets/1/6/Guarding-Our-Future.pdf>.

Toffler Associates. *Five Critical Threats to the Infrastructure of the Future*. Manchester, MA: Toffler Associates, 2008. <http://www.somanco.com/documents/Five%20Critical%20Infrastructure%20Threats.pdf>.

George Mason University, The Center for Infrastructure Protection and Homeland Security, *The CIP Report*, 10, no. 1 (July 2011).

<http://tuscany.gmu.edu/centers/cip/cip.gmu.edu/wp-content/uploads/2013/06/CIPHS_TheCIPReport_July2011_GlobalSupplyChain.pdf>.

**lesson 14 topic: written project presentations**

**1. Lesson Goals/Objectives:**

* Provide a concise analysis of a key critical infrastructure security and resilience risk assessment or management issue and provide recommendations for improvement (Problem-Discussion-Recommended Solution format).
* Provide a concise synopsis of a recommended risk assessment and management strategy for a specific infrastructure system or sector.
* Provide constructive feedback to peers on their analysis.

**2. Discussion Topics:**

* Presentations.

**3. Required Reading:**

As required for research papers and presentations.

Paul, Richard and Linda Elder. *The Miniature Guide to Critical Thinking: Concepts and Tools*. Foundation for Critical Thinking, (2009). <http://think.hanover.edu/Resources/MiniGuidetoCT.pdf>.

**lesson 15 topic: written project presentations and course wrap-up**

**\*\*special activity: final research papers are due via e-mail prior to class.**

**1. Lesson Goals/Objectives:**

* Provide a concise analysis of a key critical infrastructure security and resilience risk assessment or management issue and provide recommendations for improvement (Problem-Discussion-Recommended Solution format).
* Provide a concise synopsis of a recommended risk assessment and management strategy for a specific infrastructure system or sector.
* Provide constructive feedback to peers on their analysis.
* Summarize and discuss lessons learned and observations from learner presentations.
* Provide a forum for learner feedback on overall course content, method of instruction, and flow.

**2. Discussion Topics:**

* Presentations.
* The future of critical infrastructure security and resilience risk assessment and management – what is needed to advance the discipline and use of risk management in critical infrastructure security?
* What needs to be done to make critical infrastructure security and resilience risk assessment and management processes and approaches more widely understood and better utilized?
* Learner Course Evaluation: course content, flow, instructional methodology, etc.

**3. Required Reading:**

As required for research paper and learner presentation.

Paul, Richard and Linda Elder. *The Miniature Guide to Critical Thinking: Concepts and Tools*. Foundation for Critical Thinking, (2009). <http://think.hanover.edu/Resources/MiniGuidetoCT.pdf>.