Course: Multidisciplinary Cyber Security Risk Management

Unit 1. Fundamentals of Risk Management

Module 1. Fundamentals of Cyber Security (CS)
- Evolution of CS
- Principles of CS
- CIA – Confidentiality, Integrity, Availability
- Vulnerabilities
  - People-Process-Technology based vulnerabilities
  - Zero-Day Vulnerability
- Threats
  - Actors
  - Tools (Types of cyber-attacks (viruses, worms, Trojan, RAT, etc.) phishing, social engineering, ransomware)
- Countermeasures
  - Cryptography, hashing, authentication, authorization, accountability

Module 2. Fundamentals of Risk Management
- Definition
- Quantitate vs Qualitative
- basics of risk and decision theory
  - elements of probability theory
  - value function
  - utility function
  - GRADUATE enterprise risk
  - GRADUATE capability and operability risk
  - GRADUATE extreme event analysis
- RM Process

Module 3. RM Tools and Techniques
- RM Tools and Techniques
  - Preliminary Hazard Analysis (PHA)
  - Hazard and Operability Analysis (HAZOP)
  - Failure Mode and Effects Analysis (FMEA)
  - Fault Tree Analysis (FTA)
  - Cause and Consequences Analysis (CCA)
  - The principle of As Low As Reasonably Practicable (ALARP)
- Integrating risk management concepts into cybersecurity risk assessments
- GRADUATE Harder assignments
Module 4. Cyber Risk Governance
Risk Governance
Complexity of cyber risk management
Legal
Political
Technical
Economic
Social

Module 5. Economic aspects of cyber security

- Introduction to economics and risk management
- Economic barriers to cyber system risk management
- Economic interventions to risk management

GRADUATE Economics of technology portfolio and cyber systems risk management

Module 6. Risk, Resilience and Decision Making

- Cyber risk vs Cyber resilience
- Risk informed decision making
- Resilience informed decision making

Unit 2. Applied Standards and Cyber Risk Management

Module 7. NIST Standards

- **Cybersecurity Framework**
- **SP 800-53** Security and Privacy Controls for Federal Information Systems and Organizations

Module 8. ISO Standards

- **ISO/IEC 27000 series** - Information Security Management System
- **ISO/IEC 31000**

Module 9. Government Standards and Regulations

- Fisma
- CSET
- DoD
- [https://www.ffiec.gov/cyberassessmenttool.htm](https://www.ffiec.gov/cyberassessmenttool.htm)
- Fedramp
- Executive orders
Module 10. Industry Standards and Best Practices
   FAIR – Risk Lens
   OCTAVE
   Security Engineering Risk Analysis (SERA) Framework
   Egrc
   Cobit?
   Committee on National Security Systems - CNSS

Unit 3. Field Skills on Cyber Risk Management

Module 11. Cyber Risk Management in Cloud Environment

Module 12. Cyber Risk Management in IoT