

The background of the slide features a dark blue field with several bright, glowing blue light trails. These trails are composed of multiple parallel lines that curve and intersect, creating a sense of motion and depth. The light trails are most prominent on the left side and extend towards the right, with some horizontal streaks across the middle.

# **Secure Sourcing of COTS Products: A Critical Missing Element in Software Engineering Education**

*Nancy R. Mead, Carnegie Mellon University*  
*Anne Kohnke, University of Detroit Mercy*  
*Dan Shoemaker, University of Detroit Mercy*

## Introduction

- Software engineering education is justifiably focused on the development of software artifacts
- According to the SWEBOOK, software engineering is: *“The application of a systematic, disciplined, quantifiable approach to the development, operation, and maintenance of software.”*
- However, the vast majority of software used in organizations is COTS.
- Often, the provenance is unknown due to the supply chain.

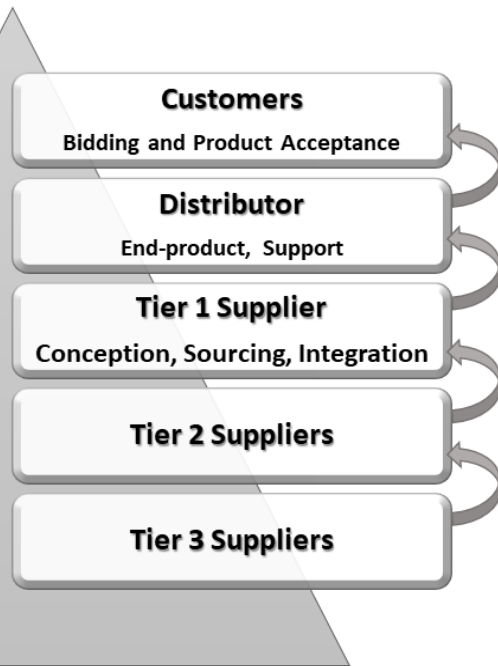
## Introduction

- The acquirer rarely knows which supplier did what work.
- The possibility of the insertion of malicious code or counterfeit parts is real.
- The emphasis in software engineering education is on good design, secure coding and effective testing.
- However, many business applications are no longer developed as stand-alone but require interoperability with a variety of other applications.

## Introduction

- Curricula do not fully address the product and programmatic interdependencies when multiple applications are used.
- There is little systematic knowledge to guide practitioners in the formal assurance that COTS products meet specifications and do NOT contain unwanted functionality.
- Specifically, the educational focus should be on how to ensure the code in COTS products hasn't been compromised through the sourcing process.

# A Process for Secure Acquisition



- Acquisition is a strategic process.
- Involves three distinct communities of practice: customer, supplier, and integrator.
- All three require a defined process to properly execute their tasks.

# Ten Principles to Regulate Performance

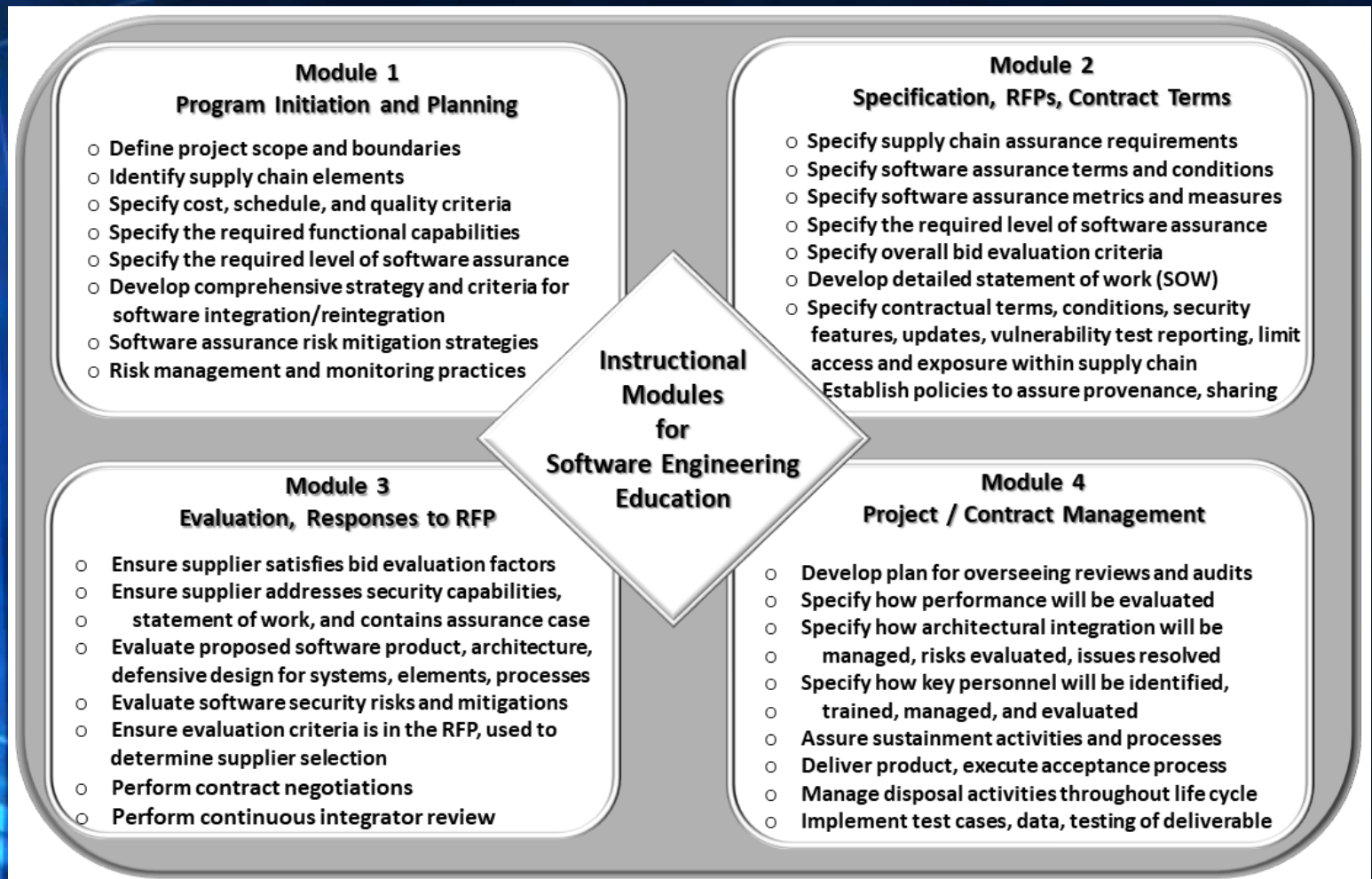


# Redesigning the Typical Software SCRM Course

- 1 Establish acquisition strategy and policy
- 2 Establish a formal acquisition process
- 3 Specify the software requirements
- 4 Identify potential suppliers
- 5 Establish contractual terms and conditions
- 6 Evaluate supplier proposals and contract
- 7 Monitor supplier progress
- 8 Certify that acceptance criteria have been satisfied
- 9 Conduct analysis of software acquisition contract, retain performance data

***Critical tasks to be included in a proposed software SCRM course***

# Course Modules Mapped to Performance and Critical Tasks





## Recommendations and Conclusion

- Given the significance, we suggest that the subject matter be encapsulated in a capstone-type course or single process-oriented course.
- For undergrad, the focus should be on fundamentals of accomplishing the topics.
- For graduate-level, emphasis should be on how to implement a unified SCRM approach as a single, coherent strategic process across all three communities of practice.
- Recommend that educators make their course materials available.

## References and Resources

- P. Bourque and R.E. Fairley, eds., "Guide to the software engineering body of knowledge, Version 3.0", IEEE Computer Society, 2014, p. xxxi.
- K. Sigler, D. Shoemaker and A. Kohnke, "Supply chain risk management: Applying secure acquisition principles to ensure a trusted technology product", CRC Press, Taylor & Francis Group, 2017.
- D. Shoemaker and N. Mead, "Building a body of knowledge for ICT supply chain risk management", Pittsburgh: Software Engineering Institute, Carnegie Mellon University, 2013.
- N. Mead and C. Woody, "Cyber security engineering: A practical approach for systems and software assurance", Addison Wesley, 2017.
- D. Shoemaker, N. R. Mead, and A. Kohnke, "Teaching secure acquisition in higher education," IEEE Security & Privacy, vol. 18, no. 4, pp. 60-66, July/Aug. 2020. DOI: 10.1109/MSEC.2020.2989644.
- D. Shoemaker and K. Sigler, "Cybersecurity: Engineering a secure information technology organization", Stamford, CT: Cengage Learning, 2015.
- D. Shoemaker, A. Kohnke, N.R. Mead, "Secure acquisition curriculum". Carnegie Mellon University, Software Engineering Institute, Digital Library, Educational Material. 2020. <https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=637101>

# Contact Information

**Nancy R. Mead**

SEI Fellow & IEEE Life Fellow  
Carnegie Mellon University  
nrmcmu@gmail.com

**Anne Kohnke**

Associate Professor  
University of Detroit Mercy  
kohnkean@udmercy.edu

**Dan Shoemaker**

Senior Research Scientist & Professor  
University of Detroit Mercy  
shoemadp@udmercy.edu