CYBE 5740
Secure Acquisition

Course Information

Prerequisites
The knowledge base for this course is evolving. It is based on a set of common best practices stipulated by national governing bodies such as NIST and ISO, as well as the most up-to-date literature in the field. Students are expected to be able to work with professional standards as well as understand common business practices. They will formulate a personal vision of the elements of acquiring secure products and services, both COTS and GOTS. This will be for the purpose of creating persistent and secure enterprise architecture.

Permission of Instructor
Given these Prerequisites students with academic background or industry experience may enroll with the permission of the instructor

Web Page: CYBE 5740
This course is fully supported from http://knowledge.udm.edu. You must enroll at the entry screen in order to access the website for the first time. All course material is on this site. Therefore all students registered in this course are required to enroll. All communication either between students or with the instructor originates from this site. The announcement board that you will see upon entry will provide all necessary updates.

Instructor Information

Name and Title

Office Location

Office Hours
by appointment via e-mail

Where to Leave Assignments
Assignments that you wish to give me can be mailed to me at the e-mail address below

E-mail

Texts and Assigned Readings

Texts

Sigler, K.E., Dan Shoemaker and Anne Kohnke, "Supply Chain Risk Management: Applying Secure Acquisition Principles to Ensure a Trusted Technology Product," Taylor and Francis, CRC Press (Internal Audit and IT Audit) 1st Edition 2018 (best purchased via Amazon)

Supporting Text (not required)

Shoemaker, Dan and Kenneth Sigler, "Cybersecurity: Engineering a More Secure IT Organization", Cengage Learning, 2014 (best accessed on Amazon)

Required Readings

Along with the reading program (published on the course calendar), I would like you to read or become familiar with (*most will be available in the "content" area of the website*):

1. ISO/IEEE 12207 -2008 02-01 (provided)
2. NISTIR 7622 Piloting Supply Chain Risk Management Practices for Federal Information Systems (provided)
3. International Standards Organization (ISO), ISO/IEC 15408 (Common Criteria) Part-1, Evaluation Criteria for IT Security – Introduction and General Model, 1999 (provided)
4. International Standards Organization (ISO), ISO/IEC 15408 (Common Criteria) Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional components (provided)
5. International Standards Organization (ISO), ISO/IEC 15408 (Common Criteria) Evaluation criteria for IT security -- Part 3: Security assurance components (provided)
6. ISO 27001 and ISO 27002 (provided as BS7799)
7. IEEE 1028-1997 Standard for Software Reviews
8. ISO/IEC 9126 – 1991 Software Product Evaluation - Quality Characteristics and Guidelines for Their Use (can be read as ISO/IEC 9126- 96)
9. IEEE 610 - Standard Glossary of Software Engineering Terminology
10. The Common Weakness Enumeration http://cwe.mitre.org/
11. Foreign Ownership, Influence or Control Investigations (FOCI) http://www.dss.mil/isp/foci/foci_info.html

Supplementary Readings

If you wish you may obtain the following additional materials.

1. Keyes, W. Noel and Steven W. Feldman, Government Contracts in a Nutshell, 5th Edition, West Publishing, Feb. 2011, ISBN: 978-0314268518
2. IEEE 829 1998 Software Test Documentation
3. IEEE 1008 1997 Standard for Software Unit Testing
4. IEEE 1042 Configuration Management Plan Guideline
5. IEEE 1045-1992 IEEE Standard for Software Productivity Metrics
6. IEEE 1062, Software Acquisition Plan
7. IEEE 1063, Software User Documentation
8. IEEE 1074 Developing Software Life Cycle Processes
9. Information Systems Audit and Control Association (ISACA), *Framework*, CobiT (fifth edition – provided)

Course Description

Description

Secure acquisition is a management/technical discipline that ensures the integrity of purchased systems and networks. Secure acquisition ensures that all purchasing risks and single points of failure are identified and mitigated to a sufficient level of satisfaction for all the stakeholders up and down the supply chain.

Secure acquisition is built around a strategic, enterprise level planning and control process. Secure acquisition is widely thought to be a function of generic risk management and technical assurance. However, because of the multifaceted environment it operates in, secure acquisition involves a much more comprehensive set of basic activities than simple software assurance. Mitigation development and deployment of a secure acquisition process involves a range of academic disciplines from governance, to specification and analysis, legal and regulatory compliance to knowledge management and testing.

Secure acquisition processes are typically industry specific in their particulars. Because of that focus of this course, which is cyber defense, the end-product will be a process engineering plan for a model case (provided) that will incorporate the lifecycle process recommendations of the ISO 12207-2008 Standard. These recommendations will be integrated into a single coherent system for the assurance of secure purchased hardware and software products and services.

Acquisition assurance is typically established at three levels in the organization, strategic processes, project infrastructure and measures for individual product assurance. We are going to examine all three of these from a top down perspective. We will move from the model that

defines and relates all of these processes, through the specific itemization of the activities and tasks embodied within this model, down to specific practices used to identify, validate, and resolve supply chain issues.

Core Learning Objectives: at the conclusion of the course the student will be able to

1. Perform a cost justification and need to acquire a secure product
2. Define a comprehensive end-to-end testing and assurance plan
3. Implement and publish an effective Request for Proposals
4. Create a secure specification of requirements
5. Execute a secure bidding process including a FICO analysis
6. Make an effective and fully enforceable contract including liquidated damages
7. Perform Monitoring and Control activities on the build process
8. Devise and execute an effective audit and control process
9. Create and execute an effective Problem Resolution Process
10. Ensure follow-up on action items has been completed
11. Inspect and accept products with assurance
12. Ensure the correctness and security of reusable code

Course Objectives

At the end of this course the student will be able to:

1. *Implement a comprehensive, well-defined, organization-wide standard-based acquisition process*
2. *Customize an appropriate set of acquisition activities for a given organization, or project by lifecycle phase*
3. *Organize, implement and manage effective acquisition operations for a complex supply chain.*

Instruction Methods

This course is conveyed through an asynchronous set of lectures posted in the content area. These are based on a PowerPoint show (also posted). In addition, students will participate in a synchronous recitation once a week. Students will execute a series of assigned labs. The product will be a formal lab report, which will serve to satisfy the requirements for each assignment. This documentation set should be appropriately detailed sufficient to unambiguously communicate how all assurance processes will be carried out. In addition, there will be a written Final.

Course Policies

Student Evaluation Procedures

Evaluation of course deliverables will be based on: *1) Conformity with the principles of SCRM management best practice (presented in lecture), 2) Complete and correct tailoring of the BOK to the particular case, and 3) A complete, correct and unambiguous presentation of findings.* Projects will be assessed based on the following criteria (relative weights in parentheses). All work products will be rated based on their demonstrated level of, *Correctness (5), Completeness (5), Unambiguousness (5), Understandability (6), Modifiability (3), Traceability (3), and Annotation (3)*. The rest of the grade will be established by*: 1.) A Final Cumulative Examination, 2.) A risk analysis for the selected case.*

Summary of Evaluation Scheme

What	When	Content	Weight
Case Exercises	Ongoing	As specified	20
Acquisition plan	Last Day of Class	As assigned	30
Discussion Board	Ongoing	As specified	20
Final	Last Day of Class	Cumulative	30

Instructions for Missed Exams and Assignments

Exams will be taken on the date specified. Assignments are due on the date specified. There are no provisions for making up either missed exams, or assignments. Some latitude will be granted for students who provide sufficient lead-time and a valid excuse.

Academic Integrity

This course falls under the provisions of the policies on academic integrity stated on page 102 of the current graduate catalogue. Any violations of this policy will result in failure.

Attendance/Lateness Policy

All assignments are due on the date specified. There will be no extensions. Students are expected to arrive on time and attend all classes and listen to all ClickMeeting sessions. Active participation in all group activities is required. A group member who fails to live up to this requirement will be subject to dismissal, after due process, and will receive a failing grade for that project assignment.

Available Support Service

Library/computer resources

Because it is fully supported by a website, this course is not library intensive. Requisite material can be accessed or downloaded from hyperlink locations provided by the instructor at the course site. Students wishing additional hardcopy material can obtain this from the McNichols library. The computer labs on both campuses are available to students during open hours.

Disability Support Services and Accommodations:

If you need an accommodation because of a disability, have emergency medical information to share, or if you need special arrangements in case the building must be evacuated, please contact:

Emilie Wetherington, Director
Disability Support Services.
McNichols Campus Library, Room 328 Email: gallegem@udmercy.edu
Phone: 313-993-1158

It is very important for students to be proactive about requesting their disability accommodations every semester. Students are encouraged to have open communication with their professors. However, it is a personal choice and never a requirement for students to disclose their disabilities to anyone except the Director of Disability Support Services, and only if they wish to request accommodations. You must be registered with Disability Support Services and your faculty must receive official notification from the DSS office before they can plan for your accommodations.

Title IX

University of Detroit Mercy is committed to fostering a safe, productive learning environment for all students. Detroit Mercy's Policy Prohibiting Sex and Gender-based Discrimination applies to sex and gender-based harassment, sexual exploitation, sexual assault, attempted sexual assault, intimate partner violence/dating violence, unwanted intimate touching, stalking, cyberstalking, and retaliation. You are encouraged to report potential sex and gender-based discrimination policy violations to Marjorie Lang, the University's Title IX coordinator, at langma@udmercy.edu or at 313.993.1802. The Title IX office is located on the 5th floor of the Fisher Administration Center on the McNichols Campus. She is available to assist you in understanding all of your options and in connecting you with all possible resources on and off campus.

Suggestions for Further Study

None of this material is required but if you want to get the maximum out of this course you should be familiar with each of them.

1. Boehm B., Improving Software Productivity, Computer, Volume 20, Number 9 September 1987
2. Boehm, Barry W., "Software Engineering Economics." IEEE Transactions on Software Engineering, Vol. SE - 10, No 1, January 1984.
3. Card, D. and E. Comer, *Why Do So Many Reuse Programs Fail?,* IEEE Software, September 1994

4. Dart, Susan A., "Achieving the Best Possible Configuration Management Solution", Crosstalk, September 1996
5. Dover, Sanford, "A Standard Response," CIO, June 1993
6. Edelstein, V., R. Fuji, C. Guerdat, and P. Sullo, "International Software Engineering Standards," *Software Engineering*, March/April,
7. Feiler, Peter, "Configuration Management Models in Commercial Environments", Tech Report CMU/SEI-91-TR-7, March 1991
8. Fenton N, *How Effective are Software Engineering Methods*, Journal of Systems and Software, Volume 22, 1993
9. Humphrey, Watts, *A Discipline for Software Engineering*, Addison-Wesley: Reading, MA, 1995
10. Humphrey Watts S., *Managing the Software Process*, Addison-Wesley: Reading, MA, 1994
11. Humphrey, Watts, and Sweet, W., *Method for Assessing the Software Engineering Capability of Contractors,* CMU/SEI-87-TR-023, Software Engineering Institute, 1987
12. ISO 9000-3 *Guidelines for the Application of ISO 9001 to the Development Supply and Maintenance of Software*, 1991
13. International Organization for Standards, *ISO/IEC 12207*, Geneva Switzerland, 1995
14. International Organization for Standards, *ISO 9000*, Geneva Switzerland, 1994
15. International Organization for Standards*, TR- 15504*, Geneva, 1998
16. Jones Capers, *The Pragmatics of Software Process Improvements*, Software Engineering Technical Council Newsletter, No. 5, Winter 1996
17. Jones, Capers, *Software Defect Removal Efficiency*, Computer, April 1996, Vol.29, #4
18. Lee, E. *Software Inspections: How to Diagnose Problems and Improve the Odds of Organizational Acceptance*, Crosstalk, Vol.10 #8 1997
19. Lim WC, *Effects of Reuse on Quality, Productivity and Economics*, IEEE Software, September 1994
20. Marshall, Alexa, "Software Configuration Management: Function or Discipline?" Crosstalk, October 1995
21. Paulk M., B. Curtis, M. Chrissis, C. Weber, "*Capability Maturity Model, Version 1.1*," Technical Report, Software Engineering Institute, Carnegie-Mellon University, 1993
22. Shoemaker, Dan, and V. Jovanovich, ISO 9000, The State of the American Software Industry, Journal of Computer Information Systems, Winter 1996
23. Software Engineering Institute, web site at www.sei.cmu.edu. 1998
24. Tomayko, James, Software Configuration Management, Carnegie Mellon, Software Engineering Institute, Pittsburgh, 1997
25. Zimmerman, Michael, "Configuration Management, Just a Fashion or a Profession", White Paper, usb GmbH, 1997
26. Cisco Systems, Inc. “Defense Agencies Meet Readiness Challenges with Commercial off the Shelf (COTS)-Based Systems” (A Cisco Intelligent Network White Paper). Cisco Systems, 2003. http://www.cisco.com/web/strategy/docs/gov/space_COTS_v2.pdf

27. Epstein, Jeremy; Matsumoto, Scott; & McGraw, Gary. “Software Security and SOA: Danger, Will Robinson!” *IEEE Security & Privacy 4*, 1 (January/February 2006).
28. International Organization for Standardization (ISO). *Standard for Systems Engineering – System Life Cycle Processes* (ISO/IEC 15288:2002). Geneva, Switzerland
29. National Infrastructure Advisory Council (NIAC). The National Strategy to Secure Cyberspace. Office of the President, 2004. http://www.whitehouse.gov/pcipb

Course Agenda

Course-Level Learning Objectives

Upon completion of this course, students will be able to:

- Students will understand the pitfalls and limitations of Global Development
- Students will understand the pitfalls and limitations of Off Shore Production
- Students will be able to describe the issues related to outsourcing development
- Students will be able to describe the issues related to outsourcing integration.
- Students will understand the pitfalls involved in Transport of ICT Components
- Students will understand the pitfalls involved in Logistics of ICT Components
- Students will prove competency in the evaluation of 3rd Party Development Practices
- Students will cite the rationale and purpose for Reverse Engineering
- Students will cite the Capabilities and Limits of Reverse Engineering in the supply chain
- Define a comprehensive end-to-end testing and assurance plan
- Implement and publish an effective Request for Proposals
- Create a secure specification of product requirements
- Execute a secure bidding process including a FICO analysis
- Make an effective and fully enforceable contract including liquidated damages
- Perform Monitoring and Control activities on the build process
- Devise and execute an effective audit and control process
- Create and execute an effective Problem Resolution Process
- Ensure follow-up on action items has been completed
- Inspect and accept products with assurance
- Ensure the correctness and security of reusable code

Unit 1: Acquisition Project Setup

Key Content Topics:

- Students will demonstrate knowledge of the global development and integration of software and system products
- Students will describe the pitfalls and advantages of offshore development • Students will be able to describe methods to mitigate known acquisition issues
- Students will be able to cite the limitations of these methods.
- Students will know and execute the steps in ICT acquisition setup

- Students will be able to demonstrate how standards such as the Orange Book can be utilized for subcontractor management
- Students will prepare a management plan including subcontractor management
- Students will Define Secure ICT SCRM
- Students will Describe the elements of the Secure SCRM Process
- Students will relate elements of the Secure SCRM Process to each other chronologically
- Students will create an acquisition/SCRM plan for a given project
- Students will document a required level of assurance for a given project

Unit Learning Objectives:

1. Demonstrate knowledge of the global development and integration of software and system products
2. Describe the pitfalls and advantages of offshore development
3. Describe methods to mitigate known acquisition issues
4. Define and justify the Need for acquisition/SCRM Initiation Practices
5. Describe the general practices associated with acquisition SCRM Initiation
6. Relate the practices of the secure acquisition process to each other chronologically
7. Describe the form and structure of a general business case for acquisition
8. Perform a business case analysis of proposed acquisition
9. Document a need to acquire based on a business case
10. Understand the purposes and application of ICT subcontracting
11. Understand the acquisition project implementation processes
12. Understand the purpose of controls in the acquisition/SCRM process
13. Understand how audit and control ensures trust in sourced purchases
14. Describe the impact of the “weakest link” on outsourced projects
15. Describe methods to ensure uniform security and control up and down a supply chain
16. Demonstrate the historical performance of outsourcing from a security perspective
17. Cite the role, of regulation in shaping governance frameworks

Required Reading:

- Curkovic, *Managing Supply Chain Risk: Integrating with Risk Management*, Chapters 2 - 3
- Shoemaker, *“Cybersecurity: Engineering a More Secure IT Organization”*, Chapter 1 -2

Web Resources:

1. ISO/IEEE 12207 -2008 02-01 (provided)

2. NISTIR 7622 Piloting Supply Chain Risk Management Practices for Federal Information Systems (provided)

Case 1: Project Initiation

The purpose of secure SCRM is to identify and mitigate any risks in the software supply chain. Please prepare a response to the following items:

For this first exercise you will define the potential functions required as well as who will supply them. You will take the following steps:

1. Identify a process in the case that you intend to support by a software application – this should include a scope, business case and assurance case statement
2. Define top-level functions required to carry out the desired process – these must be coherent (e.g., logically related and complete)
3. Decompose the top-level functions into a second level of component functions
4. Decompose the second level functions into a third level of component functions (e.g., formulate a component tree)
5. Assign a (imaginary) supplier for each component at all tiers – these will be assumed to be subcontracted relationships (e.g., the work will be done by a subcontractor directly employed by the higher-level entity)

Unit Two: Specification and Bidding

Key Content Topics:

- Students will define assurance needs and requirements for a given project
- Students will explicitly specify project assurance needs
- Students will explicitly specify project assurance requirements
- Students will specify management and technical capability requirements
- Students will explicitly document management requirements
- Students will explicitly document technical capability requirements
- Students will execute appropriate analyses to determine whether to contract out work
- Students will execute e analyses to determine how much of the work to contract out
- Students will align a business case with security requirements
- Students will align a business case with functional requirements
- Identify responsibilities of all organizations involved in the process

Unit Learning Objectives:

1. Perform an analysis to determine (maximum) potential risk
2. Perform an analysis to differentiate value of achieving different levels of reduced risk
3. Document value of achieving different levels of reduced risk
4. Define an acceptably realistic project scope based on cost and technical feasibility
5. Define a distinctive project boundary
6. Specify cost schedule, and quality criteria for a given scope
7. Specify the required functional capabilities for a given scope
8. Specify the required level of software assurance for a given scope
9. Document project scope
10. Define and document the responsibilities of all process participants

Required Reading:

- Curkovic, Managing Supply Chain Risk: Integrating with Risk Management, Chapter 4
- Shoemaker, "Cybersecurity: Engineering a More Secure IT Organization", Chapter 3-4 • International Standards Organization (ISO), ISO/IEC 15408 (Common Criteria) Part-1, Evaluation Criteria for IT Security – Introduction and General Model, 1999 (provided)
- International Standards Organization (ISO), ISO/IEC 15408 (Common Criteria) Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional components (provided)
- International Standards Organization (ISO), ISO/IEC 15408 (Common Criteria) Evaluation criteria for IT security -- Part 3: Security assurance components (provided)

Case 2: Acquisition/SCRM Project Risk Analysis

Utilize the forms taken from NISTIR 7622 (provided). Identify and assess risks against the Base Practices for that Community of Practice to obtain an overall risk rating for each participant in the supply chain. The risk rating can be used to prioritize the risks. To facilitate this process, it is useful to use a generic checklist as a stimulus to identify what risks may affect components, or participants. This is provided for this course.

Examine the portion of the project you have chosen to control. Use the assessment tool provided to evaluate the current status of the relevant community of practice. Then develop mitigation strategies and timelines to address the risk where the level of risk is not acceptable.

Unit 3: Standard Frameworks and Compliance Control (Session Three July 16, 18 and 23)

Key Content Topics:

- Students will know how to select appropriate contract terms
- Students will base terms on cost, schedule, and performance risks
- Students will document assurance requirements through contract language
- Students will know how to establish process for testing and evaluation of requirements • Students will know how to establish remediation options to ensure final acceptance.
- Students will know how to Identify and mitigate outsourcing considerations

Unit Learning Objectives:

1. Define what constitutes a constraint on the process
2. Know how to perform a FOCI to identify constraints
3. Know how to utilize risk assessment to identify constraints
4. Know how to utilize protection profiles were appropriate
5. Be able to document all relevant constraints
6. Be able to specify risk mitigation requirements for each constraint

Required Reading:

- "Cybersecurity: Engineering a More Secure IT Organization", Chapters 5 and 7
- ISO 27001 and ISO 27002 (provided as BS7799)
- IEEE 1028-1997 Standard for Software Reviews
- ISO/IEC 9126 – 1991 Software Product Evaluation - Quality Characteristics and Guidelines for Their Use (can be read as ISO/IEC 9126- 96)
- IEEE 610 - Standard Glossary of Software Engineering Terminology
- The Common Weakness Enumeration http://cwe.mitre.org/
- Foreign Ownership, Influence or Control Investigations (FOCI) http://www.dss.mil/isp/foci/foci_info.html

Case 3: Adequacy of Acquisition Practice

Explanation of the Assessment Process

The purpose of this assignment is to evaluate the current capability maturity of your ICT supply acquisition security practice. The assessment will determine areas in your organization where proper acquisition risk management is being practiced, as well as the relative maturity of those

practices The goal is to generate a nominal ranking of capability maturity based on a universal scale of process performance.

Selection of Appropriate Communities of Practice

The total set of potential practices encompasses the recommendations of NIST IR 7622 "Supply Chain Risk Management Practices for Federal Information Systems" (NIST, 2010), which is the most authoritative current reference for proper ICT supply chain risk management practice. The practices in NIST IR 7622 apply differently within three different communities of practice; Acquirers, Suppliers and Integrators. Therefore, depending on the role your organization plays you may be required to fill out this assessment tool for more than one community of practice. And as a consequence, three different assessment tools have been provided representing each of those notional communities.

How to Do the Assessment

Using the Case, please address each practice in the instrument (provided) as an individual, unique requirement. Provide your best estimate of the level of execution for each of these requirements. Depending on your judgment place a [number] "1" in the column that most appropriately describes the level of execution of each of the individual practices. At the bottom of the instrument you will find a grand-total ranking for the degree of process capability for each of the columns. That sum is the total number of responses for each maturity level. You will be able to roughly determine your organization's level of capability maturity based on where the bulk of your responses fall. This will allow you to judge the relative maturity of your overall supply chain risk management process, as well as the areas where some improvement may be required.

Unit 4: Supplier Evaluation

Key Content Topics:

- Student will evaluate supplier qualifications for secure product development
- Student will evaluate supplier qualifications for integrating secure products
- Student will evaluate supplier history in the practice of good product engineering
- Student will determine whether the supplier employs known "hackers"
- Student will determine level of foreign ownership, influence, or control
- Student will evaluate impacts of foreign ownership, influence or control
- Student will describe the elements of the supplier risk management process
- Student will develop strategies for mitigation of supplier risks by acquirer

Unit Learning Objectives:

1. Perform market research to determine if required capabilities are available
2. Describe all project lifecycle actions for risk management

3. Determine the level of sensitivity of information processed by the software
4. Identify and describe vulnerability and threat status of product
5. Identify and describe vulnerability and threat status of supplier
6. Develop a standard risk-based categorization scheme for risk
7. Ensure supplier software assurance risk monitoring
8. Implement a strategy for monitoring the risk mitigation strategies
9. Assess whether those strategies result in acceptable outcomes

Required Resources:

- "Cybersecurity: Engineering a More Secure IT Organization", Chapters 8 and 9

Optional Resources:

1. IEEE 1028-1997 Standard for Software Reviews
2. ISO/IEC 9126 – 1991 Software Product Evaluation - Quality Characteristics and Guidelines for Their Use (can be read as ISO/IEC 9126- 96)
3. IEEE 610 - Standard Glossary of Software Engineering Terminology
4. The Common Weakness Enumeration http://cwe.mitre.org/

Case 4: Supplier Capability Evaluation (due NLT Thursday August 8th)

Using the Supplier Checklist from NIST-IR 7622 (provided) assess the competency of the organization in the case. You must provide a complete plan as well as the outcome of the assessment (score). Maturity levels will be assessed using the scale provided across the top of the instrument. For each practice please rate its execution as: Not Done Performed, Managed, Predictable, and Optimizing. The various common features of each capability level will help guide your decision in placing your response.

Incomplete: The Incomplete level has no common features. There is general failure to perform the base practices. There are no easily identifiable work products or outputs of the practice.

Performed: Base practices of the process are generally performed. Individuals within the organization recognize that an action should be performed, and there is general agreement that this action is performed when required. The performance of these base practices is ad-hoc and is not rigorously planned, or tracked. Performance depends on individual knowledge and effort. There are identifiable work products for the process Work testify to the performance of the practice.

Managed: The performance of the process is planned and tracked and executed systematically within the organization. Base practices are performed according to a well-defined process using approved methods which are tailored versions of standard, documented processes.

Predictable: Execution of the process is fully reliable because detailed measures of performance are collected and analyzed. This leads to a quantitative understanding of process capability and an improved ability to predict performance. Performance is objectively managed. The quality of work products is quantitatively known.

Optimizing: Quantitative process effectiveness and efficiency goals (targets) for performance are established, based on the business goals and system assurance case of the organization. Continuous process improvement against these goals is enforced by quantitative data that is obtained from the execution of the defined processes as well as from piloting innovative ideas and technologies.

Unit 5: Acceptance and Sustainment

Key Content Topics:

- Student will know how to do Product Assurance Process Planning
- Student will know how to Perform all due diligence actions for process risk management
- Student will know how to develop FOCI mitigations
- Student will know how to Include product assurance criteria in the estimate
- Student will know how to prepare a Strategy and develop Criteria for Reuse
- Student will describe a way to decide whether to Employ Reusable Code
- Students will describe advantage of deducing design features via reverse engineering
- Students will describe disadvantage of deducing design features via reverse engineering
- Student will consider the impacts and implications of reverse engineering to source
- Student will consider the impacts of not having source to fix problems
- Student will describe how visibility and control over source can be reverse engineered
- Student will Describe software-related security risks of reusable code
- Student will list Controls required to ensure security of reusable software
- Student will Mitigate common acquirer concerns for Reuse
- Student will Describe a valid process to ensure limitations to software reuse are known
- Student will Describe a valid process to ensure that limitations are clearly stated
- Student will Describe a valid process to ensure correctness of Risk mitigation strategies
- Student will Describe legal obligations if a supplier uses reusable code
- Student will Itemize a valid set of measures for Assurance of development practices
- Student will Develop Software Assurance Risk Mitigation Strategies • Student will Describe and justify a logical set of risk mitigation strategies.
- Student will Establish a baseline level of software assurance as part of the SCRM

Unit Learning Objectives:

1. Specify all project lifecycle actions for risk management

2. Document all project lifecycle actions for risk management
3. Assurance of proposal evaluation by qualified individuals
4. Estimation of cost of risk management over the entire life cycle
5. Identify relevant types of reusable product elements
6. Describe role of open source software
7. Describe role of other reusable code (free software)
8. Describe role of value-added products or services
9. Describe the reverse engineering process for product understanding
10. Describe the security issues associated with product reverse engineering
11. Describe the advantages of reusable code
12. Visible source code benefits from community review
13. Describe how to ensure reusable software against risk
14. Describe a valid process for vulnerability reporting
15. Describe a valid process for construction and deployment of patches
16. Describe a valid process for construction and deployment of new versions
17. Describe valid process to confirm assurance level prior to integration
18. Describe a valid process to confirm assurance level after integration
19. Describe a valid process for financial analysis of life cycle costs.
20. Describe conditions for approval of use of reusable code
21. State pedigree requirements
22. Understand and state an appropriate level of acceptable vulnerability
23. Describe a valid patch management strategy
24. Describe the basis for negotiated liabilities for loss or damage
25. Describe testing required to produce the equivalent of an assurance case
26. Control over software reuse among subsidiaries
27. Evaluation of Reusable Software
28. Build an assurance case
29. Integrate reuse assurance case with overall assurance arguments

Required Resources:

"Cybersecurity: Engineering a More Secure IT Organization", Chapters 7 and 12

- Software Security and Reverse Engineering, http://www.infosecwriters.com/text_resources/pdf/software_security_and_reverse_engineering.pdf

Optional Resources:

1. ISO/IEC 9126 – 1991 Software Product Evaluation - Quality Characteristics and Guidelines for Their Use (can be read as ISO/IEC 9126- 96)
2. The Common Weakness Enumeration http://cwe.mitre.org/