Carnegie Mellon University
Software Engineering Institute

SEI Education and Training Catalog

The Best Training for Today's Software, Systems, and Cybersecurity Challenges

Get the Edge You Need

Learn to acquire, develop, operate, and sustain software systems that are innovative, affordable, enduring, and trustworthy by completing our training courses at the Software Engineering Institute (SEI). Our many learning options are sure to meet your learning goals.

Our software and cybersecurity experts, recognized for their contributions to field-based research, have practical experience that enables them to develop and teach our courses. Acquire critical skills through hands-on tasks and real-world scenarios. Immerse yourself in current and practical courses that challenge your assumptions and help you explore new and unexpected ideas.

Contents

Flexible Course Delivery Options

Our course delivery options help you follow the best training approach given your schedule and preferred learning style. All training is presented by our expert instructors and includes a carefully integrated mix of lectures, exercises, and discussions where you also learn from fellow professionals.

In eLearning, you register for the course and move at your own pace according to your own schedule.

In classroom training, you visit an SEI facility to participate in the course. We also offer on-site training, where our instructors travel to your location and teach the course to your team.

In virtual classroom, you participate in a live, online session with SEI instructors and other attendees.

How to Register

Individuals

Register for most courses on the SEI website (sei.cmu.edu/training).

Groups

Schedule private, on-site classroom training or take advantage of group discounts for online training. Contact us (course-info@sei.cmu.edu) for more information.

Recognize Your Educational Accomplishments

An SEI Professional Certificate acknowledges your professional accomplishments in a technical curriculum. Each certificate requires that you work through a carefully designed set of courses. Requirements differ among technical areas and programs. As an SEI Professional Certificate holder, you receive an official certificate from the SEI and the option of having your name and accomplishment published on the SEI website.

These courses fulfill the requirements for one or more professional certificate programs.

More Information

Find more information about SEI education and training on the SEI website:

sei.cmu.edu/training

We offer public domain Continuing Educational Units (CEUs) for most of our training courses. We calculate CEUs based on the total class hours using the ANSI/AICET standard, which awards 1 CEU for 10 hours of instruction.

Training courses provided by the SEI are not academic courses for academic credit toward a degree. Any certificates provided are evidence of the completion of the courses and are not official academic credentials.

Software Architecture

Software Architecture: Principles and Practices

Two-Day Course • eLearning • Classroom

sei.cmu.edu/training/v07.cfm

In this course, you learn the essential concepts of software architecture and the importance of the business (or mission) context for system design. The course introduces software architectures in a real-world setting and uses "industrial-strength" case studies to cover key technical and organizational issues.

Who should attend? those who design, develop, or manage the construction of software-reliant systems

Topics covered include what a software architecture is and why it's important, the architecture influence cycle, the relationships among system qualities and software architectures, architectural patterns and tactics and their relationship to system qualities, and more.

Documenting Software Architectures

Two-Day Course • eLearning • Classroom

sei.cmu.edu/training/v18.cfm

In this course, you learn effective software architecture documentation practices that meet the needs of the stakeholder community in the context of prevailing prescriptive models, including the Rational Unified Process (RUP), the Siemens Four Views software approach, the IEEE 1471-2000 standard, and the Unified Modeling Language (UML).

Who should attend? software architects and lead designers, software technical managers and engineers who may be expected to use architecture documentation

Topics covered include the basic principles of sound technical documentation, a stakeholder- and view-based approach to documenting software architectures, views available for documenting an architecture, and more.

Software Architecture Design and Analysis

Two-Day Course • Classroom

sei.cmu.edu/training/p34.cfm

In this course, you learn concepts for effectively designing and analyzing a software architecture. You apply the SEI Attribute-Driven Design (ADD) software architecture design method and are introduced to the SEI Quality Attribute Workshop (QAW), the SEI Architecture Tradeoff Analysis Method (ATAM), and several lightweight evaluation techniques.

Who should attend? practicing software architects, and designers and developers of software-reliant systems

Topics covered include the essential considerations in any architectural design process, how to elicit critical quality attributes, the ADD method for designing an architecture, the role of architecture evaluation, and how to use these methods in a software development lifecycle.

Designing Modern Service-Based Systems

One-Day Course • Classroom

sei.cmu.edu/training/p124.cfm

In this course, you learn the main types of service-oriented architecture (SOA) design elements and technologies. You study comparisons of microservices and the monolithic deployment model, and learn about security, transaction management, and service deployment.

Who should attend? software and application architects, developers who use service technologies in their solutions, and project managers and IT personnel responsible for SOA implementations

Topics covered include basic concepts related to SOA and service-based solutions; what is necessary to be successful with SOA; and main types of components found in service-based solutions, including REST services, platform-specific services, message brokers, and API gateways.

Design Guidelines and Patterns for Microservices

Two-Day Course • Classroom

sei.cmu.edu/training/p125.cfm

In this course, you gain the essential knowledge needed to understand the microservices landscape, including the seven guidelines for service-oriented designs. You study strategies that help you realize each design guideline. In the design lab, you evaluate designs based on guidelines and create new designs using different patterns and other design strategies.

Who should attend? software and application architects and developers who use service and microservice technologies in their solutions

Topics covered include microservices and microservice architecture style**;** design guidelines for successful service-based solutions; and strategies, including several design patterns that can be used to realize the service-orientation guidelines.

Managing Technical Debt of Software

One-Day Course • eLearning • Classroom

sei.cmu.edu/training/v37.cfm

In this course, you learn about the concept of technical debt—when a design or construction approach is taken that is expedient in the short term but increases complexity and cost in the long term. You study how technical debt manifests, accumulates, and affects the enterprise. You also learn to assess, measure, and manage the technical debt landscape.

Who should attend? software professionals who design, develop, or manage the construction of software-reliant systems and who need insights into how to successfully manage technical debt

Topics covered include learning the technical debt definition framework, making technical debt visible, understanding when it accumulates, paying it back, and living with it.

Big Data: Architectures and Technologies

One-Day Course • eLearning • Classroom

sei.cmu.edu/training/v32.cfm

In this course, you learn the relationships that exist among application software, data models, and deployment architectures, and how technology selection relates to them. You learn about distributed data storage, access infrastructure, and the architecture tradeoffs needed to achieve scalability, consistency, availability, and performance.

Who should attend? architects, technical stakeholders involved in the development of big-data applications, product managers, development managers, and systems engineers

Topics covered include what big data is, how and why it has evolved, and the technologies that address its complexities; the basics of distributed systems; the quality attributes important in distributed systems and how they are achieved in practice; and more.

Advanced Software Architecture Workshop

Two-Day Course • Classroom

sei.cmu.edu/training/p102.cfm

In this course, you are introduced to an architecture that has undergone evaluation through the SEI Architecture Tradeoff Analysis Method (ATAM). You learn to select a problematic scenario for a system, examine weak points of its software architecture, decide appropriate mitigations, review proposed changes in groups, and revise the architecture as required.

Who should attend? software architects and software lead designers who want to practice what they've learned in the SEI software architecture curriculum or want to prepare for a project that requires major architecture improvements

Topics covered include improving architecture through a defined process, analyzing and planning architecture tasks, improving an existing architecture design, conducting a scenario-based peer review, and preparing documentation to support conformance of the implementation.

Architecture Tradeoff Analysis Method (ATAM) Evaluator Training

Two-Day Course • Classroom

sei.cmu.edu/training/p31.cfm

In this course, you learn to conduct a software architecture evaluation using the ATAM, including how to apply it to software architectures. You perform an ATAM evaluation exercise with guidance from your instructors to systematically evaluate software architectures for fitness of purpose and to expose architectural risks.

Who should attend? those responsible for or involved in the evaluation of software architectures, such as software architects, system architects, software designers, and system designers; and those who want to participate in SEI-authorized ATAM evaluations

Topics covered include quality attributes and their role in software architectures, quality attribute tradeoffs, and why architecture analysis is important.

Modeling System Architectures Using the Architecture Analysis and Design Language (AADL)

Five-Day Course • Classroom

sei.cmu.edu/training/p72.cfm

In this course, you learn the fundamental model-based concepts for engineering real-time, embedded software systems by defining and documenting software and system architectures and validating system quality attributes. This course builds on the SAE AADL (Architecture Analysis and Design Language) standard for engineering real-time, embedded software systems.

Who should attend? software developers; those tasked with validating embedded, real-time system performance; technical managers; managers; and software/system architects

Topics covered include the value of model-based engineering, choices for system representation and modeling, core elements of the AADL, quantitative validation of quality attributes through the analysis of system architecture, and more.

AADL in Practice Workshop

Five-Day Course and Two-Day Workshop • Classroom

sei.cmu.edu/training/p128.cfm

In this course and follow-on workshop, you learn and apply the modeling techniques necessary to adopt AADL. You are introduced to MBE methods and AADL tools in the course; you then put those skills to use in a realistic modeling and analysis scenario in the workshop with expert SEI guidance.

Who should attend? those who design and develop software; those tasked with validating embedded, real-time system performance; technical managers, managers, and software/system architects looking for a solid overview of system and software modeling; those who make decisions about developing or acquiring real-time, embedded systems

Topics covered include reviewing the existing example problem, defining modeling and analysis objectives, discussing practical modeling approaches, creating and analyzing models, and reviewing/critiquing work produced.

Software Product Lines

Two-Day Course • eLearning • Classroom

sei.cmu.edu/training/v08.cfm

In this course, you learn the basic concepts of software product lines and the essential technical and management practices needed to succeed with them. Using case studies, you learn how to apply product line techniques and determine if a product line approach is right for your organization.

Who should attend? software engineers and technical managers interested in effective reuse strategies or who are adopting or using a software product line approach

Topics covered include the essential activities involved in fielding software product lines, product line practice patterns that aid in product line adoption, a product line diagnostic method, and more.

Cyber Intelligence

Cyber Intelligence for Decision Makers

Two-Hour Course • eLearning

sei.cmu.edu/training/v33.cfm

In this course, you learn a non-technical approach to cyber intelligence, how important it is to understand cyber intelligence in the context of your organization, and how to use cyber intelligence to improve the way you make decisions. You study a structured approach you can use to understand, evaluate, and assess cyber intelligence vulnerabilities.

Who should attend? executives, managers, and team leaders

Topics covered include the role of cyber intelligence in your organization, your organization's cyber threat environment, potential risk factors and preventive measures, core competencies and skills recommended for an intelligence team, and more.

Incident Handling

Fundamentals of Incident Handling

Five-Day Course • Classroom

sei.cmu.edu/training/p26.cfm

In this course, you learn the basic tasks and skills that that enable you to perform your daily work as an incident handler. In particular, you learn how to gather information to handle an incident, how to perform analysis and response tasks for various sample incidents, and how to identify potential problems while working in a CSIRT.

Who should attend? CSIRT technical staff with one to three months of experience, CSIRT staff who want to benchmark their CSIRT processes and skill sets, and anyone who wants to learn about basic incident handling functions and activities

Topics covered include the technical issues related to commonly reported attack types, the issues involved in providing a CSIRT service, how to analyze and assess the impact of computer security incidents, and more.

Advanced Incident Handling

Five-Day Course • Classroom

sei.cmu.edu/training/p23B.cfm

In this course, you learn how to detect and respond to computer security threats and attacks targeted at a variety of operating systems and architectures. You also practice identifying and analyzing events and propose appropriate response strategies, and learn how to respond to system compromises at the privileged level.

Who should attend? CSIRT technical staff with three to six months of incident handling experience, and system and network administrators responsible for identifying and responding to security incidents

Topics covered include detecting and characterizing various attack types, effectively responding to privileged and major events and incidents within your CSIRT, analyzing artifacts left on a compromised system, exploring new developments in computer forensics, and more.

Creating a Computer Security Incident Response Team (CSIRT)

One-Day Course • Classroom

sei.cmu.edu/training/p25.cfm

In this course, you learn the issues and decisions you need to address when establishing a CSIRT. You develop an action plan for implementing a CSIRT in your organization. You study organizational models for CSIRTs, the services that a CSIRT can provide, and the resources and infrastructure needed to support one.

Who should attend? current and prospective CSIRT managers, C-level managers interested in establishing a CSIRT, and other staff who interact with CSIRTs

Topics covered include developing and implementing a new CSIRT; addressing issues related to assembling a responsive, effective team; using organizational models for a new CSIRT; and more.

Managing Computer Security Incident Response Teams (CSIRTs)

Three-Day Course • Classroom

sei.cmu.edu/training/p28.cfm

In this course, you develop a pragmatic view of the issues you face when operating an effective CSIRT. You gain insight into the work that CSIRT staff may be expected to handle as well as the basics of the incident handling process and the types of tools and infrastructure it needs to be effective.

Who should attend? CSIRT managers and other staff who interact with CSIRTs and want to learn more about how they operate

Topics covered include the policies and procedures needed to establish a CSIRT; processes for detecting, analyzing, and responding to computer security events and incidents; key components for sustaining CSIRT operations; and more.

Introduction to Computer Forensics

Two-Hour Course • eLearning

sei.cmu.edu/training/v34.cfm

In this course, you learn about the tasks, processes, and technologies used to identify, collect, preserve, and analyze data so that it can be used in a judiciary setting. You also learn to apply good forensic practices and understand how routine actions can affect the forensic value of data.

Who should attend? those involved in the collecting, storing, and analyzing computer systems and network data, including digital forensics, systems security analysis, and incident response

Topics covered include developing an investigative process for a digital forensic investigation; methods of focusing investigations; preparing for incident response, including network reconnaissance and network traffic analysis; and more.

Advanced Digital Forensics

Ten-Hour Course • eLearning

sei.cmu.edu/training/v34.cfm

In this course, you learn the details of the entire investigative process and how to determine "who did it." You improve your ability to piece together the components of a digital investigation. Using a simulated lab environment, you refine your investigative skills by responding to a realistic scenario.

Who should attend? those involved in collecting, storing, and analyzing computer systems and network data, including digital forensics, systems security analysis, and incident response

Topics covered include preparing for and responding to incidents on victim and suspect systems, conducting network reconnaissance and analyzing network traffic, identifying sources of evidentiary value in various evidence sources, and more.

Advanced Forensic Response and Analysis

Three-Day Course • Classroom

sei.cmu.edu/training/p103.cfm

In this course, you learn how to conduct incident response and forensic analysis investigations. You study common evidence-collection measures and forensic analysis steps, methods for organizing analyses to identify relevant evidentiary data, and common areas of evidentiary value to further your investigations.

Who should attend? computer forensic professionals who understand core forensic and information technology principles and students who conduct incident response, intrusion, or other computer forensic investigations

Topics covered include preparing for an intrusion investigation, using best practices for responding to incidents and collecting data, applying methods for analyzing victim and perpetrator systems, identifying malicious applications, and more.

Overview of Creating and Managing Computer Security Incident Response Teams (CSIRTs)

One-Day Course • Classroom

sei.cmu.edu/training/p68.cfm

In this course, you benefit from a consolidated view of information from two other CERT courses: *Creating a CSIRT* and *Managing CSIRTs.* You learn best practices in planning, implementing, operating, and evaluating a CSIRT.

Who should attend? CSIRT and C-level managers, project leaders, CSIRT team members, system and network administrators, security staff, human resources staff, media or public relations staff, law enforcement, and legal counsel

Topics covered include differentiating between incident management and incident response activities, identifying the type of work that CSIRT managers and staff may be expected to handle, and more.

Network & Software Security

Secure Coding in C and C++

Four-Day Course • eLearning • Classroom

sei.cmu.edu/training/v35.cfm

In this course, you learn common programming errors in C and C++ and how these errors can lead to code that is vulnerable to exploitation. You study security issues intrinsic to the C and C++ programming languages and their associated libraries.

Who should attend? C and C++ developers

Topics covered include how coding errors can be exploited, effective mitigation strategies, how to thwart buffer overflows and stack-smashing attacks, how to eliminate integer-related problems, how to avoid I/O vulnerabilities, and more.

Secure Coding in Java

Four-Day Course • eLearning • Classroom

sei.cmu.edu/training/v36.cfm

In this course, you learn about common programming errors in Java and how they can lead to code that is vulnerable to exploitation. You study security issues intrinsic to Java programming languages and their associated libraries.

Who should attend? Java developers

Topics covered include how coding errors can be exploited, effective mitigation strategies, how to avoid injection attacks, how to prevent race conditions while avoiding deadlock, how to throw and catch exceptions at the right time, and more.

Security Requirements Engineering Using the SQUARE Method

One-Day Course • Classroom

sei.cmu.edu/training/p104.cfm

In this course, you learn about security requirements engineering and the SQUARE method. You learn the SQUARE steps in detail. For each step, you participate in a team case study and discuss follow-on research and transition activities. You learn how SQUARE helps organizations build security into the early stages of the production lifecycle.

Who should attend? software managers, technical leads, software engineers, requirements engineers, and security specialists

Topics covered include the importance of developing security requirements when you develop functional requirements, why methods to identify functional requirements may not work directly for security requirements, methods for security risk analysis, and more.

Software Assurance Methods in Support of Cyber Security

One-Day Course • Classroom

sei.cmu.edu/training/p108.cfm

In this course, you study four critical software assurance areas: security requirements, software supply chain assurance, mission thread analysis, and measurement. You are exposed to concepts and resources for addressing software security assurance across the acquisition and development lifecycles.

Who should attend? software managers, technical leads, software and lead engineers, software and system acquisition experts, and program/project managers

Topics covered include the challenges of software assurance; key concepts and methods for security risk analysis and measurement, security requirements elicitation, mission thread analysis, and supply chain risk analysis; best practices for software assurance; and more.

DevOps in Practice Workshop

One-Day Course • Classroom

sei.cmu.edu/training/p115.cfm

In this course, you get a comprehensive, hands-on review of DevOps topics and processes and learn techniques for project planning, development, and deployment. You are exposed to reference architectures and get hands-on experience with continuous integration tools and practices.

Who should attend? technical managers, technical leads, developers, QA engineers, release/deployment engineers, and operational support staff of software development teams

Topics covered include best practices used by DevOps industry leaders, how modern automation and tooling solve common problems in software development and delivery, how to best begin a DevOps transformation within your own organization, and more.

Secure DevOps Process and Implementation

Five-Hour Course • eLearning

sei.cmu.edu/training/v38.cfm

In this course, you learn DevOps principles, processes, and techniques for project planning, development, and deployment. You are exposed to reference architectures and use cases on continuous integration tools and practices, including technical demonstrations and practical scenarios.

Who should attend? software development technical managers, technical leads, developers, QA engineers, release engineers, and operational support staff

Topics covered include the common pitfalls and missteps of DevOps; adapting DevOps theories, practices, and tools to meet your particular business needs; and providing measurable value to your organization.

Vulnerability Response Capability Development

One-Day Course • Classroom

sei.cmu.edu/training/p123.cfm

In this course, you learn the key issues, processes, and decisions that must be made to enable your organization to respond to vulnerabilities reported in its products. You develop an action plan to use as a starting point for planning and implementing your vulnerability response capability.

Who should attend? managers and project leaders, current and prospective product security managers, and project leaders interested in establishing or starting a vulnerability response capability

Topics covered include requirements, policies, and procedures for establishing a vulnerability response capability; various organizational models used; and the types of resources and infrastructures needed to support a team.

Information Security for Technical Staff

Five-Day Course • eLearning • Classroom

sei.cmu.edu/training/v21.cfm

In this course, you learn to protect the security of your organization's information assets and resources; techniques for managing risks, threats, policy, system configurations, availability, and personnel; and how to work with TCP/IP security and cryptography in the context of incident response.

Who should attend? technical staff members who manage or support networked information systems

Topics covered include key concepts of the TCP/IP protocol suite, how to gather information on networked systems, attack methods perpetrated against network systems, an approach for staying current with information security, and more.

Applied Cybersecurity, Incident Response, and Forensics

Five-Day Course • Classroom

sei.cmu.edu/training/p107.cfm

In this course, you improve your knowledge and skills for administering and securing information systems and networks. You study topics such as vulnerability assessment, systems administration, network monitoring, incident response, and digital forensics. You participate in team exercises modeled from real-world scenarios.

Who should attend? technical staff members who manage or support networked information systems

Topics covered include installing and configuring network access control technologies and intrusion detection sensors, using technology to monitor the status/availability of network services, safely collecting and securing sensitive incident response data, and more.

Managing Enterprise Information Security: A Practical Approach for Achieving Defense-in-Depth

Three-Day Course • Classroom

sei.cmu.edu/training/p61.cfm

In this course, you learn the conceptual foundations of information security. You are introduced to the CERT Defense-in-Depth Framework. You synergistically apply the eight operationally focused and interdependent management components of the framework to a fictitious organization's IT enterprise.

Who should attend? technical staff members

Topics covered include understanding the CERT Defense-in-Depth Framework, examining IT operations for information assurance (IA) threats and vulnerabilities, and applying the framework to improve the security posture of IT operations.

Risk Assessment & Insider Threat

Insider Threat Overview: Preventing, Detecting, and Responding to Insider Threats

Five-Hour Course • eLearning

sei.cmu.edu/training/v26.cfm

In this course, you learn the different types of insider threats, the threats they pose to critical assets, how to recognize technical and behavioral indicators, and various insider threat mitigation strategies.

Who should attend? insider threat program team members and program managers

Topics covered include the prevalence of insider threat activity and the damage it can cause, how to recognize and avoid unintentional insider threats, the best practices for insider threat mitigation, and more.

Building an Insider Threat Program

Seven-Hour Course • eLearning

sei.cmu.edu/training/v27.cfm

In this course, you learn about the organizational models and necessary components of an insider threat program. You learn how to identify the key stakeholders to involve, create, and roll out an implementation plan, and identify needed policies and procedures.

Who should attend? insider threat program team members and program managers

Topics covered include identifying the staff and skills needed for an insider threat program operational team, identifying the type of governance and management support needed to sustain the formal program, and more.

Insider Threat Program Manager: Implementation and Operation

Three-Day Course • Classroom

sei.cmu.edu/training/p110.cfm

In this course, you learn a process roadmap you can use to build an insider threat program. You study techniques and methods for developing, implementing, and operating program components. You learn how to establish insider threat detection and prevention programs to satisfy government mandates or guidance.

Who should attend? insider threat program team members and managers

Topics covered include identifying critical assets and protection schemes, identifying data sources and priorities for data collection, improving security awareness, identifying competencies for insider threat team staff, and more.

Insider Threat Vulnerability Assessor Training

Three-Day Course • Classroom

sei.cmu.edu/training/p112.cfm

In this course, you develop the skills and competencies needed to perform an insider threat vulnerability assessment. You learn how to plan and conduct an assessment to identify issues, design tactical countermeasures, and formulate a strategic action plan for long-term risk mitigation.

Who should attend? those interested in performing an insider threat vulnerability assessment

Topics covered include developing a data collection plan, interviewing staff to corroborate indicators, entering evidence into the Joint Assessment Tool (JAT), scoring capabilities, defending assessment results, and more.

Insider Threat Awareness Training

One-Hour Course • eLearning

sei.cmu.edu/training/v29.cfm

In this course, you learn about insider threats and how to protect your organization's critical assets. You also learn how your work can be affected by insider threats.

Who should attend? all employees (especially those with a security clearance), senior executives, insider threat program team members, insider threat program managers, contractors and subcontractors, and suppliers and business partners

Topics covered include the common motivations of malicious insiders, different types of insider threats, the impacts of insider threats, how you can be targeted by malicious individuals and external adversaries, and more.

Assessing Information Security Risk Using the OCTAVE Approach

Three-Day Course • eLearning • Classroom

sei.cmu.edu/training/v22.cfm

In this course, you learn to perform information security risk assessments using the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) approach. You study OCTAVE's prescribed activities for risk identification, analysis, and response.

Who should attend? security professionals, business continuity planners, compliance personnel, risk managers, and others who must satisfy security standard requirements

Topics covered include the connection between information security, business continuity, IT operations, and operational risk management; tailoring OCTAVE to meet unique organizational needs; and more.

Measuring What Matters: Security Metrics Workshop

Two-Day Course • Classroom

sei.cmu.edu/training/p117.cfm

In this course, you develop specific business goals and learn about the questions, indicators, and actionable metrics that you can implement in your organization to improve how you manage operational risks, particularly cybersecurity risks.

Who should attend? directors and managers of operational risk management, information technology (IT), cybersecurity/information security, IT and cybersecurity compliance, and IT and cybersecurity auditors

Topics covered include refining strategic or business objectives to meet S.M.A.R.T.E.R. (Specific, Measureable, Achievable, Relevant, Time-Bound, Evaluated, Reviewed) criteria and initiate the GQIM (Goals, Questions, Indicators, Metrics) process; identifying a set of goals based on your business objectives; and more.

Introduction to the CERT Resilience Management Model

Three-Day Course • Classroom

sei.cmu.edu/training/p66.cfm

In this course, you learn how to manage operational resilience using the CERT Resilience Management Model (CERT-RMM). You also learn how to evaluate your current security, business continuity, and IT operations practices and determine which ones are working and which ones to replace.

Who should attend? security and business continuity professionals; process improvement professionals, particularly those looking to operations processes; enterprise and operational risk management professionals; and anyone interested in applying a maturity model approach to managing operational resilience

Topics covered include CERT-RMM process areas, how CERT-RMM is used to appraise an organization's capability for managing operational resilience, and how to plan process improvement in your organization.

Smart Grid Maturity Model (SGMM) Navigator Training

Two-Day Course • Virtual Classroom

sei.cmu.edu/training/p109.cfm

In this course, you learn Smart Grid Maturity Model (SGMM) Navigation in preparation for becoming an SEI-Certified SGMM Navigator. You explore a Smart Grid implementation using an interactive virtual classroom and follow a case study that simulates all aspects of the SGMM Navigation process.

Who should attend? system integrators, consultants, vendors, and those who plan to assist utilities through SGMM planning and implementation

Topics covered include planning and conducting a survey workshop for a utility, validating and analyzing SGMM Compass survey data to produce insightful findings, planning and conducting an aspirations workshop, and more.

Acquisition Support

Leading SAFe/Agile in Government

Three-Day Course • Classroom

sei.cmu.edu/training/p126.cfm

In this course, you are introduced to the interactions that government program offices have with developers who are using Agile team methods and the Scaled Agile Framework approach to develop government systems. You also learn about the Agile and Lean concepts that software developers use.

Who should attend? government staff who (1) interact with contractor SAFe/Agile teams, (2) are considering adopting SAFe/Agile methods, or (3) will be interacting in an Agile enterprise; development contractors interested in understanding how government organizations expect to interact with them in Agile development settings

Topics covered include SAFe principles and application; Agile basics (e.g., lifecycles, the Agile Manifesto, methods, and practices); the new product-owner role of government; Agile insight and oversight; SAFe portfolio management; Agile in the larger ecosystem; and enabling an Agile culture.

Acquisition Essentials for Software-Reliant Systems

One-Hour Course • eLearning

sei.cmu.edu/training/v23.cfm

In this course, you learn three fundamental software acquisition topics: software requirements, software architecture, and software testing. You study stories from real acquisition programs that show the significance of these three topics.

Who should attend? acquisition program leaders and staff

Topics covered include the unique challenges of software-reliant systems and the knowledge needed to manage software-reliant acquisition programs and keep them on track by proactively recognizing symptoms and implementing recovery strategies.

Twenty Questions to Assess Your Program's Chances of Success

One-Hour Course • eLearning

sei.cmu.edu/training/v24.cfm

In this course, you learn risk management concepts and the 20 key drivers that comprise the SEI risk-based method for assessing complex projects: the Mission Diagnostic Protocol. You study these drivers and how the assessment of a program using these drivers creates a profile of a program's chances of success.

Who should attend? managers and program staff interested in project and program management as well as those interested in learning how to assess and manage risk in developmental and operational settings

Topics covered include risk management concepts and terminology, the key drivers of program success, how drivers can be used when assessing a program's systemic risk, and using the Standard Driver Workbook to assess a program's success.

Data Rights and DoD Acquisition

Three-Hour Course • Virtual Classroom

sei.cmu.edu/training/v25.cfm

In this course, you learn what to consider with respect to data rights when acquiring software. You also learn why data rights are important, a risk-based method to help determine what rights are needed, and how to include data rights in your acquisitions.

Who should attend? program managers, request for proposal (RFP) developers, software engineers, contract staff, engineering staff, logistics staff (sustainment issues), DoD acquisition policy makers, and software development contractors

Topics covered include recognizing the complexity of managing data rights in a DoD environment, identifying Defense Federal Acquisition Regulations (DFARs) and contract clauses that impact data rights, using a data rights strategy in RFP evaluations, and more.

COTS Software Product Evaluation for Practitioners

Two-Day Course • Classroom

sei.cmu.edu/training/p51.cfm

In this course, you learn about the process and techniques for evaluating commercial off-the-shelf (COTS) products in software-intensive systems. You also use best practices based on real-world case studies to learn about a process framework for COTS software product evaluations.

Who should attend? practitioners who are charged with conducting COTS software product evaluations

Topics covered include understanding the impact of COTS products on the system development process, developing COTS software evaluation criteria, using a COTS software evaluation process that addresses inherent tradeoffs, and more.

Practical Risk Management: Principles and Methods

Two-Day Course • Classroom

sei.cmu.edu/training/p78.cfm

In this course, you learn practical methods for managing risk across the lifecycle and supply chain. You learn a practical approach to risk management, and you examine several ways to implement this approach.

Who should attend? project managers; lead engineers; software engineers; risk managers and others performing risk management activities; EPG and SEPG members; change or technology transition agents; and those from related disciplines, such as quality assurance, acquisition, security, and IT

Topics covered include tailoring the Mosaic risk management methodology to your needs and constraints, applying Mosaic risk management methods to evaluate an existing risk management practice for completeness and effectiveness, and more.

Measurement & Analysis

Implementing Goal-Driven Measurement

Three-Day Course • Classroom

sei.cmu.edu/training/p06.cfm

In this course, you learn to identify and define indicators and measures that support your organization's business, process improvement, and project goals. The methods you learn are relevant to product development, process improvement, and project management.

Who should attend? project managers; process managers; SEPG members; process improvement working group members; software measurement team members; and those who need reliable information to guide acquiring, supporting, planning, or tracking software systems

Topics covered include defining measures and indicators that support the measurement requirements of ISO standards, such as ISO 15939; starting and leading measurement activities in the context of software process improvement programs; and more.

Analyzing Project Management Indicators

Three-Day Course • Classroom

sei.cmu.edu/training/p07b.cfm

In this course, you learn how to use measurement to analyze project performance, manage schedules and resources, and communicate project status and changes. You learn how to use metrics to plan technical work, integrate related business goals, and address stakeholder issues in an overall project plan.

Who should attend? project managers and those supporting managers of software-intensive system development, maintenance, and acquisition

Topics covered include defining indicators based on what a project manager needs to know, using measurement to support decision making, using measurement data to communicate more clearly to project stakeholders, and more.

Improving Process Performance Using Six Sigma

Five-Day Course • Classroom

sei.cmu.edu/training/p49b.cfm

In this course, you use an improvement framework for analyzing data to help you make more informed business decisions. Leveraging best practices, such as Six Sigma and Goal-Driven Software Measurement, you also learn how to balance project and process performance, quality, schedule, and cost.

Who should attend? software engineering process group members; process improvement working group members; software measurement team members; Six Sigma black belts, green belts, or belt candidates; project managers; and process managers

Topics covered include exploring and navigating data to understand project, process, and product behavior, relationships, and trends; using analysis methods to remove special causes of variation and stabilize processes; and more.

Designing Products and Processes Using Six Sigma

Five-Day Course • Classroom

sei.cmu.edu/training/p56b.cfm

In this course, which builds on the statistical concepts from the *Improving Process Performance Using Six Sigma* course, you learn advanced and powerful analytical methods and get extensive hands-on practice with problems faced by product development teams.

Who should attend? product development leaders (systems, hardware, software) and members of engineering process groups, quality improvement groups, process action teams, or appraisal teams

Topics covered include implementing a variety of measurement techniques to dramatically improve requirements engineering and solution selection, using advanced measurement techniques to model uncertainty and predict cost and schedule performance, and more.

Implementing Goal-Driven Measurement Instructor Training

Three-Day Course • Classroom

sei.cmu.edu/training/a17.cfm

In this course, you learn to lead the *Implementing Goal-Driven Measurement* course and teach students a method for identifying and defining indicators and measures that directly support their organizations' business goals related to product development, process improvement, and project management.

Who should attend? experienced trainers and measurement professionals who are interested in becoming SEI-certified instructors of the *Implementing Goal-Driven Measurement* course

Topics covered include concepts and issues to emphasize in each course module, how to provide critiques of course exercise results, how to respond to methodology questions from students, and more.

Improving Process Performance Using Six Sigma Instructor Training

Two-Day Course • Classroom

sei.cmu.edu/training/a23.cfm

In this course, you learn to present the *Improving Process Performance Using Six Sigma (IPPSS)* course and introduce students to a method for driving improvement based on performance using a method and toolbox originating with the Six Sigma Define, Measure, Analyze, Improve, and Control (DMAIC) paradigm.

Who should attend? experienced trainers and measurement professionals who want to become SEI-certified instructors of the *Improving Process Performance Using Six Sigma* course

Topics covered include providing critiques of IPPSS course exercise results, providing feedback that aligns with and reinforces concepts that are integral to the course approach and highlights the correct and incorrect application of the DMAIC method, and more.

Designing Products and Processes Using Six Sigma Instructor Training

Two-Day Course • Classroom

sei.cmu.edu/training/a24.cfm

In this course, you learn to teach the *Designing Products and Processes Using Six Sigma (DPPSS)* course and introduce students to the method and toolbox (Define-Measure-Analyze-Design-Verify [DMADV]), which can be used for designing products and processes based on performance.

Who should attend? experienced trainers and measurement professionals who want to become SEI-certified instructors of the DPPSS course

Topics covered include presenting DPPSS course modules to students, evaluating course exercise results and giving feedback that aligns with and reinforces course concepts, providing feedback on the application of the DMADV method, and more.

Team Software Process

Team Software Process (TSP) Executive Strategy Seminar

One-Day Course • Classroom

sei.cmu.edu/training/p22.cfm

In this course, you learn the key concepts and principles of the Team Software Process (TSP) and Personal Software Process (PSP) from a management perspective. You receive the information needed to begin introducing and applying the TSP in your organization.

Who should attend? executives; middle managers responsible for software development or maintenance; managers responsible for software quality and assurance, software engineering process groups, systems or hardware engineering, documentation, or finance

Topics covered include how the TSP can effectively improve software development activities and provide positive motivation for engineers and project teams, using the TSP to address current and future software needs, and more.

Team Software Process (TSP) Team Member Training

2.5-Day Course • Classroom

sei.cmu.edu/training/p16b.cfm

In this course, you learn the foundational concepts of the PSP and TSP. You study how to measure size, time, and defects in you work; how to use a personal planning framework to plan and track your tasks; and how to use a quality strategy to manage defects in your work and be prepared to participate on a TSP team.

Who should attend? system, hardware, and test engineers; technical writers; trainers; and others who participate on a TSP project

Topics covered include the TSP launch process; how to be a productive participant of a launch; using weekly meetings, inspections, checkpoints, and postmortems to manage and maintain self-directed teams; and more.

Leading a Development Team

Three-Day Course • Classroom

sei.cmu.edu/training/p17b.cfm

In this course, you learn how to manage quantitatively to complete projects on schedule, within budget, and with all requirements met. You study the knowledge and skills that Team Software Process (TSP) leaders need to effectively lead and coach development teams.

Who should attend? first-level software development managers, software project managers, software team leaders, and supervisors

Topics covered include how operational procedures and data can improve software development; key behaviors for successfully leading and coaching teams; quantitatively managing projects using effective cost, schedule, and quality measures; and more.

Personal Software Process (PSP) Fundamentals

Five-Day Course • Classroom

sei.cmu.edu/training/p18b.cfm

In this course, you learn how to apply PSP methods to your personal work process and how to participate on a Team Software Process (TSP) team. You study how to measure and analyze your personal software process, use process data to improve your personal performance, and apply PSP methods to other structured tasks.

Who should attend? software engineers, software engineering students, software engineering instructors, software quality management instructors, and third-party vendors of software engineering or quality training

Topics covered include the PSP process-based approach for developing software, measuring and analyzing your personal software processes, and managing and reducing defects through your software processes.

Personal Software Process (PSP) Advanced

Five-Day Course • Classroom

sei.cmu.edu/training/p19b.cfm

In this course, you learn high-level Personal Software Process (PSP) and Team Software Process (TSP) concepts. You study how to optimize your process performance by applying approaches that include a defined estimating process, tracking and predicting with earned value, quality techniques for improving product and programmer productivity, and more.

Who should attend? software engineers, software engineering students, software engineering instructors, software quality management instructors, and third-party vendors of software engineering or quality training

Topics covered include analyzing your current performance, improving your performance based on that analysis, and extending PSP methods with best practices.

Personal Software Process (PSP) Instructor Training

Five-Day Course • Classroom

sei.cmu.edu/training/p20.cfm

In this course, you learn to teach the Personal Software Process (PSP) and put it into practice. You study how to effectively teach the PSP, how to grade student assignments and analyze the resulting data, and how to introduce the PSP into an organization.

Who should attend? potential software engineering instructors, potential software quality management instructors, and third-party vendors of software engineering or quality training

Topics covered include introductory concepts of the Team Software Process (TSP).

Team Software Process (TSP) Coach Training

Five-Day Course • Classroom

sei.cmu.edu/training/p21.cfm

In this course, you learn to launch and coach effective Team Software Process (TSP) teams. You study the key concepts and principles of the TSP from an operational and procedural perspective and learn how to recognize and effectively address common problems that occur in TSP launches.

Who should attend? potential TSP coaches, team leaders, and third-party vendors who want to provide TSP training and coaching to their clients

Topics covered include using tools that support the launch process, coaching a TSP team between launches and checkpoints, the coach's rights and obligations under the TSP Product Suite agreement, and more.

Training Certificates

CERT Certificate in Digital Forensics

Two Courses

sei.cmu.edu/training/v34.cfm

As a system and network administrator, you must understand the fundamentals of computer forensics. You must also apply good forensic practices to routine administrative procedures and alert verification, and know how routine actions can adversely affect the forensic value of data. Such an awareness greatly enhances your effectiveness when responding to security alerts and other routine matters. This certificate builds on your existing skills by teaching you the essential elements of digital forensics. You study how to be prepared to approach both routine and unusual events in a systematic, forensic manner.

Who should attend? experienced system and network computer professionals who collect, store, and analyze computer systems and network data, and conduct digital forensics, systems security analysis, or incident response activities

CERT Insider Threat Program Manager (ITPM) Certificate

Three Courses and an Exam

cert.org/insiderthreat/insider-threat-program-manager-itpm-certificate.cfm

Earning this certificate helps you develop a formal insider threat program in your organization. You study insider threat planning, identification of internal and external stakeholders, components of an insider threat program, insider threat team development, strategies for effective communication of the program, and how to effectively implement and operate the program.

Who should attend? insider threat program managers and team members

CERT Insider Threat Vulnerability Assessor (ITVA) Certificate

Three Courses and an Exam

cert.org/insiderthreat/insider-threat-vulnerability-assessor-itva-certificate.cfm

Earning this certificate enables you to help organizations gain a better understanding of their insider threat risk and identify and manage that risk. You study an assessment methodology that measures how prepared organizations are to prevent, detect, and respond to insider threats.

Who should attend? insider threat program managers and candidate assessors

CERT Incident Response Process Professional Certificate

Two Courses

sei.cmu.edu/training/certificates/security/response.cfm

Earning this certificate prepares you to be a member of a computer security incident response team (CSIRT). You study incident handling, and common and emerging attacks that target a variety of operating systems and architectures. You gain insight into the work of a CSIRT member and other topics related to incident handling, including intruder threats, the nature of incident response activities, and how incident handlers can respond to system compromises.

Who should attend? CSIRT technical personnel

CERT Information Security Professional Certificate

Two Courses

sei.cmu.edu/training/certificates/security/infosecurity.cfm

Earning this certificate prepares you with practical techniques for protecting the security of your organization's information assets and resources and increases your ability to administer and secure information systems and networks. You study security issues, technologies, and recommended practices at increasing layers of complexity, beginning with concepts and proceeding to technical implementations.

Who should attend? technical staff members who manage or support networked information systems

CISO-Executive Certificate Program

Six-Month Program

heinz.cmu.edu/school-of-information-systems-and-management/cio-institute/chief-information-security-officer-executive-education-and-certification-program/index.aspx

Earning this certificate enables you to develop and manage information security (IS) resources, and design and implement organizational IS policies. You study everything from security metrics to enterprise security governance to crisis communication to information security law. You learn to address the issues that chief information security officers (CISOs) face and have an opportunity to interact with peer CISOs.

Who should attend? CISOs or equivalent position

CRO Certificate Program

Five-Month Program

heinz.cmu.edu/school-of-information-systems-and-management/cio-institute/chief-risk-officer-certificate-program/index.aspx

Earning this certificate provides domain leaders with the latest skills and best practices in risk management. You focus on what chief risk officers (CROs) need to be successful and develop your risk management skills. You learn strategies for communicating risks to executive leadership and learn about tools you can use to analyze and address enterprise risks.

Who should attend? CROs or equivalent position

CERT Secure Coding in C and C++ Professional Certificate

Two Courses and an Exam

sei.cmu.edu/training/v35.cfm

Earning this certificate helps you increase the security of your software and reduce vulnerabilities in the programs you develop using C and C++. You learn to recognize common programming errors that lead to software vulnerabilities, thwart buffer overflows and stack-smashing attacks that exploit insecure string manipulation logic, avoid the incorrect use of dynamic memory management functions, eliminate integer-related problems, and avoid I/O vulnerabilities, including race conditions.

Who should attend? C and C++ software developers

CERT Secure Coding in Java Professional Certificate

Two Courses and an Exam

sei.cmu.edu/training/V36.cfm

Earning this certificate helps you increase the security of your software and reduce vulnerabilities in the programs you develop using Java. You learn to recognize common programming errors that lead to software vulnerabilities, avoid injection attacks, understand Java's memory model, recognize when to throw and catch exceptions, understand how common errors can be exploited, employ mitigation strategies to prevent introducing common errors, and avoid I/O vulnerabilities.

Who should attend? Java software developers

SEI Software Architecture Professional Certificate

Three Courses and an Exam

sei.cmu.edu/training/certificates/architecture/professional.cfm

Earning this certificate provides you with the breadth and depth you need to understand software architecture concepts and practices. Beginning with software architecture fundamentals, you gain experience in effective architecture documentation, design, and analysis techniques, and then learn how these techniques can be used in adopting a product line approach to software.

Who should attend? designers and developers of software-reliant systems

SEI Architecture Tradeoff Analysis Method (ATAM) Evaluator Certificate

Two Courses and an Exam

sei.cmu.edu/training/certificates/architecture/atame.cfm

Earning this certificate prepares you for performing SEI-authorized ATAM architecture evaluations. You study the essential concepts of software architecture and the ATAM, an effective method for systematically evaluating software architectures for fitness of purpose.

Who should attend? software professionals responsible for or involved in the evaluation of software architectures

SEI Service-Based Architecture Professional Certificate

Three Courses and an Exam

sei.cmu.edu/training/certificates/architecture/service-based-architecture.cfm

Earning this certificate provides you with the software architecture and SOA concepts and practices that you need to successfully architect service-based systems. The courses that support this certificate apply to service-based systems in general and do not favor any specific platforms, tools, or products.

Who should attend? software professionals responsible for designing, developing, or deploying service-based systems; technical and project managers responsible for migrating legacy systems or managing SOA or microservice implementations

Course Credit
Training courses provided by the SEI are not academic courses for academic credit toward a degree. Any certificates provided are evidence of the completion of the courses and are not official academic credentials.

About the SEI

For more than three decades, the Software Engineering Institute (SEI) has been helping government and industry organizations acquire, develop, operate, and sustain software systems that are innovative, affordable, enduring, and trustworthy. We serve the nation as a federally funded research and development center (FFRDC) sponsored by the U.S. Department of Defense (DoD) and are based at Carnegie Mellon University, a global research university annually rated among the best for its programs in computer science and engineering.

Contact Us

SOFTWARE ENGINEERING INSTITUTE
4500 FIFTH AVENUE
PITTSBURGH, PA 15213-2612

W sei.cmu.edu/training/
T 412.268.7622 | 888.201.4479
E course-info@sei.cmu.edu