Brief 110: ISTQB/ASTQB – Certification Overview

Outline Last Updated: 10/26/21

Course Description

Test and Evaluation (T&E) training and certification prepares T&E professionals with the skills, knowledge, and abilities to carry out their work in an effective and efficient manner. Leading in certifications for software testing globally is the International Software Testing Qualifications Board (ISTQB) and the American Software Testing Qualifications Board (ASTQB), which represents ISTQB in the U.S. The ASTQB maintains a portfolio of 18 software testing certifications that cover a broad set of topics across a large body of knowledge which are discussed in a one day class.

Topics include fundamental testing knowledge and techniques, to advanced topics on test automation, performance testing, and model-based testing. Each certification is derived from a body of knowledge that includes a syllabus and glossary. This course will go through the different certifications which are available, the value they each provide, and recommendations on how these certifications can benefit T&E professionals across a variety of work assignments and as part of T&E professional development.

Course Goals/Objectives

A T&E professional who successfully completes this course will:

1. Understand the breadth and depth of the ISTQB/ASTQB certification offerings
2. Understand which ISTQB/ASTQB certifications should be considered for T&E professionals, based on their role
3. Summarize the benefits that ISTQB/ASTQB can provide programs in greater efficiency and effectiveness
4. Understand the progression of certifications to fit a given role and meet short- and long-term goals
5. Understand where ISTQB/ASTQB certifications support DevSecOps
6. Understand how ISTQB/ASTQB certifications help advance the testing profession
7. Understand the role certifications play in addressing testing challenges

Course Duration

The one (1) day class format may include the full course content (8 hours), condensed content (4 hours), or reduced content (2 hours) is customarily delivered as a virtual live instructor event. A course outline can be provided in order to define overall requirements and course length.

Course Materials

Electronic copies of slides will be provided.

Target Audience

In general, we recommend this course for DoD executive-level (e.g., SES), test and evaluation (T&E) leadership, and Project Management Office (PMO) personnel and other decision makers. In particular, we recommend the certification training described in this overview to PMO Program Managers, Project Managers, Chief Developmental Tester (CDT), Lead Developmental Test Organization (LDTO), T&E professionals (e.g., Test Managers, Test Leads) and T&E technical practitioners (Test Analysts, Test Engineers) and others working in DT, OT, and IT.

Student Standards

All students must be familiar with and adhere to the standards of academic freedom, non-attribution and academic integrity. Below are the definitions for these terms:

Academic Freedom

- You may express your opinions concerning current or proposed policies, regulations and procedures openly, honestly, and professionally
- You may not attack the character, personality or other personal attributes of any individual
- Academic freedom must be tempered by good judgment to refrain from making offensive remarks, unfounded opinions, or irresponsible statements.

Non-Attribution

- What you say in class will not be attributed to you if and when your thoughts or ideas are repeated outside of class
- All guest speakers, students, and permanent-party personnel are prohibited from divulging the identity of any particular speaker, whether a guest speaker, faculty member, or student, for the purpose of attributing to that speaker any specific remarks or statements, including but not limited to offensive remarks and irresponsible statements

DSO 220: DevSecOps – T&E Professional Syllabus

Outline Last Updated: 10/26/21

Course Description

DevSecOps is changing the way in which DoD develops, deploys, and protects software intensive software and systems. This new paradigm requires an understanding of processes, tools, and techniques for Test and Evaluation (T&E). This two-day course, designed for senior T&E professionals (e.g., Test Managers, Test Leads), will define the DevSecOps software lifecycle as applied to Department of Defense software intensive systems. Goals and activities for each phase of the DevSecOps lifecycle will be covered. Software tools and automation used across DevSecOps will be demonstrated.

The course will follow each phase within the DevSecOps lifecycle and highlight senior T&E professional opportunities for applying Scientific Test and Analysis Techniques (STAT), software test automation, and security testing, within DevSecOps. Senior T&E professionals will leave this course with knowledge and understanding of what DevSecOps represents and how this affects T&E activities.

Course Goals/Objectives

A senior T&E professional who successfully completes this course will:

8. Understand the necessity and advantage of DevSecOps for DoD software intensive systems
9. Describe in detail overall concepts within DevSecOps
10. Define ways in which Scientific Test and Analysis Techniques (STAT) can bring rigor, efficiency, and effectiveness to a program using DevSecOps
11. Define goals and activities surrounding STAT, security, and automation tools within each following cycles: Development (Dev), Operations (Ops), Security (Sec)
12. Understand relevance and importance of phases within the Security (Sec) Cycle
13. Understand topics and concepts that will facilitate conducting a DevSecOps gap analysis
14. Understand the broad set of software tools used in DevSecOps and opportunities for automation

Course Duration

Two (2) day class format (7 hours class time and 1 hour lunch break) can delivered in-person (onsite) or as a virtual live instructor event.

Course Materials

Electronic copies of slides will be provided.

Target Audience

In general, we recommend this course for senior T&E professionals (e.g., Test Managers, Test Leads).

Student Standards

All students must be familiar with and adhere to the standards of academic freedom, non-attribution and academic integrity. Below are the definitions for these terms:

Academic Freedom

- You may express your opinions concerning current or proposed policies, regulations and procedures openly, honestly, and professionally
- You may not attack the character, personality or other personal attributes of any individual
- Academic freedom must be tempered by good judgment to refrain from making offensive remarks, unfounded opinions, or irresponsible statements.

Non-Attribution

- What you say in class will not be attributed to you if and when your thoughts or ideas are repeated outside of class
- All guest speakers, students, and permanent-party personnel are prohibited from divulging the identity of any particular speaker, whether a guest speaker, faculty member, or student, for the purpose of attributing to that speaker any specific remarks or statements, including but not limited to offensive remarks and irresponsible statements

DSO 230: DevSecOps – T&E Technical Practitioner Syllabus

Outline Last Updated: 10/26/21

Course Description

DevSecOps is changing the way in which DoD develops, deploys, and protects software intensive software and systems. This new paradigm requires an understanding of processes, tools, and techniques for Test and Evaluation (T&E). This three-day course, designed for T&E technical practitioners (e.g., Test Analysts, Test Engineers) and Test Teams (DT, OT, IT), will define the DevSecOps software lifecycle as applied to Department of Defense software intensive systems. Goals and activities for each phase of the DevSecOps lifecycle will be covered. Software tools and automation used across DevSecOps will be demonstrated and individuals will participate in live, hands-on, exercises that demonstrate the various tools and technology that are used throughout DevSecOps.

The course will follow each phase within the DevSecOps lifecycle and highlight T&E technical practitioner opportunities for applying Scientific Test and Analysis Techniques (STAT), software test automation, and security testing, within DevSecOps. T&E technical practitioners will leave this course with knowledge and understanding of what DevSecOps represents, how this affects T&E technical activities.

Course Goals/Objectives

A senior T&E professional who successfully completes this course will:

15. Understand the necessity and advantage of DevSecOps for DoD software intensive systems
16. Describe in detail overall concepts within DevSecOps
17. Define ways in which Scientific Test and Analysis Techniques (STAT) can bring rigor, efficiency, and effectiveness to a program using DevSecOps
18. Define goals and activities surrounding STAT, security, and automation tools within each following cycles: Development (Dev), Operations (Ops), Security (Sec)
19. Understand relevance and importance of phases within the Security (Sec) Cycle
20. Understand topics and concepts that will facilitate conducting a DevSecOps gap analysis
21. Experience the broad set of software tools used in DevSecOps and opportunities for automation

Course Duration

Three (3) day class format (7 hours class time and 1 hour lunch break) can delivered in-person (onsite) or as a virtual live instructor event.

Course Materials

Electronic copies of slides will be provided.

Target Audience

In general, we recommend this course for T&E technical practitioners (e.g., Test Analysts, Test Engineers) working in Developmental Testing (DT), Integrated Testing (IT), and Operational Testing (OT).

Student Standards

All students must be familiar with and adhere to the standards of academic freedom, non-attribution and academic integrity. Below are the definitions for these terms:

Academic Freedom

- You may express your opinions concerning current or proposed policies, regulations and procedures openly, honestly, and professionally
- You may not attack the character, personality or other personal attributes of any individual
- Academic freedom must be tempered by good judgment to refrain from making offensive remarks, unfounded opinions, or irresponsible statements.

Non-Attribution

- What you say in class will not be attributed to you if and when your thoughts or ideas are repeated outside of class
- All guest speakers, students, and permanent-party personnel are prohibited from divulging the identity of any particular speaker, whether a guest speaker, faculty member, or student, for the purpose of attributing to that speaker any specific remarks or statements, including but not limited to offensive remarks and irresponsible statements

DSO 310 DevSecOps – Project Management Syllabus

Outline Last Updated: 10/26/21

Course Description

DevSecOps is changing the way in which DoD develops, deploys, and protects software intensive software and systems. This new paradigm requires an understanding of processes, tools, and techniques for Test and Evaluation (T&E). This half-day course, designed for Project Management Office (PMO) personnel (e.g., PM, CDT, LDTO), will introduce the DevSecOps software lifecycle as applied to Department of Defense software intensive systems. A high level overview and summary of the goals, tools, and activities within each phase of the DevSecOps lifecycle will be covered.

The course will follow each phase within the DevSecOps lifecycle and highlight PMO leadership opportunities for applying Scientific Test and Analysis Techniques (STAT), software test automation, and security testing, within DevSecOps. PMO leadership will leave this course with knowledge and understanding of what DevSecOps represents, how this affects T&E activities, and the necessary questions to conduct a proper DevSecOps T&E gap analysis.

Course Goals/Objectives

A leader who successfully completes this course will:

22. Understand the necessity and advantage of DevSecOps for DoD software intensive systems
23. Describe a high-level overview of major concepts within DevSecOps
24. Summarize ways in which Scientific Test and Analysis Techniques (STAT) can bring rigor, efficiency, and effectiveness to a program using DevSecOps
25. Summarize goals and activities surrounding STAT, security, and automation tools within each following cycles: Development (Dev), Operations (Ops), Security (Sec)
26. Understand the phases within the Security (Sec) Cycle
27. Articulate necessary questions to ask in order to conduct a proper DevSecOps gap analysis

Course Duration

Four (4) hour class format is customarily delivered as a virtual live instructor event.

Course Materials

Electronic copies of slides will be provided.

Target Audience

In general, we recommend this course for Project Management Office (PMO) personnel. In particular, we recommend this course for PMO Program Managers, Project Managers, Chief Developmental Tester (CDT), and the Lead Developmental Test Organization (LDTO).

Student Standards

All students must be familiar with and adhere to the standards of academic freedom, non-attribution and academic integrity. Below are the definitions for these terms:

Academic Freedom

- You may express your opinions concerning current or proposed policies, regulations and procedures openly, honestly, and professionally
- You may not attack the character, personality or other personal attributes of any individual
- Academic freedom must be tempered by good judgment to refrain from making offensive remarks, unfounded opinions, or irresponsible statements.

Non-Attribution

- What you say in class will not be attributed to you if and when your thoughts or ideas are repeated outside of class
- All guest speakers, students, and permanent-party personnel are prohibited from divulging the identity of any particular speaker, whether a guest speaker, faculty member, or student, for the purpose of attributing to that speaker any specific remarks or statements, including but not limited to offensive remarks and irresponsible statements

DSO 410: DevSecOps – Executive Level Syllabus

Outline Last Updated: 10/26/21

Course Description

DevSecOps is changing the way in which DoD develops, deploys, and protects software intensive systems. This new paradigm requires an understanding of processes, tools, and techniques for Test and Evaluation (T&E). This two hour course, designed for DoD executive-level (e.g., SES) and test and evaluation (T&E) leadership, introduces the concepts of the DevSecOps software lifecycle as applied to Department of Defense software intensive systems. A high level overview and summary of the goals, activities, and supporting technology within each phase of the DevSecOps lifecycle will be covered.

The course will follow each phase within the DevSecOps lifecycle and highlight T&E leadership opportunities for applying Scientific Test and Analysis Techniques (STAT), software test automation, and security testing, within DevSecOps. T&E leadership will leave this course with knowledge and understanding of what DevSecOps represents, how this affects T&E activities, and the necessary questions to conduct a proper DevSecOps T&E gap analysis.

Course Goals/Objectives

An executive who successfully completes this course will:

28. Understand the necessity and advantage of DevSecOps for DoD software intensive systems
29. Describe a high-level overview of major concepts within DevSecOps
30. Summarize goals and activities surrounding STAT, security, and automation tools within each following cycles: Development (Dev), Operations (Ops), Security (Sec)
31. Understand the phases within the Security (Sec) Cycle
32. Understand areas to assess in order to identify DevSecOps gaps

Course Duration

Two (2) hour class format is customarily delivered as a virtual live instructor event.

Course Materials

Electronic copies of slides will be provided.

Target Audience

In general, we recommend this course for SES-equivalent or higher. In particular, we recommend this course for DoD executive-level test and evaluation (T&E) leadership.

Student Standards

All students must be familiar with and adhere to the standards of academic freedom, non-attribution and academic integrity. Below are the definitions for these terms:

Academic Freedom

- You may express your opinions concerning current or proposed policies, regulations and procedures openly, honestly, and professionally
- You may not attack the character, personality or other personal attributes of any individual
- Academic freedom must be tempered by good judgment to refrain from making offensive remarks, unfounded opinions, or irresponsible statements.

Non-Attribution

- What you say in class will not be attributed to you if and when your thoughts or ideas are repeated outside of class
- All guest speakers, students, and permanent-party personnel are prohibited from divulging the identity of any particular speaker, whether a guest speaker, faculty member, or student, for the purpose of attributing to that speaker any specific remarks or statements, including but not limited to offensive remarks and irresponsible statements