Software Engineering Institute

A Systematic Approach for Assessing Workforce Readiness

Christopher Alberts
David McIntire

August 2014

TECHNICAL REPORT
CMU/SEI-2014-TR-009

CERT Division

http://www.sei.cmu.edu

Carnegie Mellon University

This material is based upon work funded and supported by Department of Homeland Security under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of Department of Homeland Security or the United States Department of Defense.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

DM-0001276

Table of Contents

List of Figures

List of Tables

Acknowledgments

We would like to thank several members of the SEI technical staff for their contributions to this work over the past few years: Robin Ruefle and Sandra Behrens for their technical contributions to the Competency Lifecycle Roadmap; Christian Roylo and Larry Rogers for providing expertise in forensic analysis; Jeff Gennari and John Ackley for providing expertise in malware analysis; Jennifer Cowley for sharing results of her research with malware analysis; and all technical staff members and students that participated in our piloting of the readiness tests for forensic data collection. We would also like to thank Irina Popova-Nowak of Booz Allen Hamilton for her technical review of our competency work; SEI technical staff member Palma Buttles-Valdez for her technical review of this report; and Sandy Shrum for her editing of this report. We would like to acknowledge the support that we received from Shawn Pindell, Daniel Stein, and Keri Nusbaum, our sponsors in the Department of Homeland Security (DHS). Finally, we would like to thank the fellows from the DHS Secretary's Honors Program for Cyber (SHPC) that participated in our piloting of the readiness tests for forensic data collection.

Abstract

Workforce effectiveness relies on two critical characteristics: competence and readiness. *Competence* is the sufficient mastery of the knowledge, skills, and abilities needed to perform a given task. It reflects how well an individual understands subject matter or is able to apply a given skill. *Readiness* is the ability to apply the total set of competencies required to perform a job task in a real-world environment with acceptable proficiency. A readiness test assesses an individual's ability to apply a group of technical and core competencies needed to perform and excel at a job task. This report describes research into workforce readiness conducted by the Computer Security Incident Response Team (CSIRT) Development and Training team in the CERT® Division of Carnegie Mellon® University's Software Engineering Institute (SEI). This report presents the Competency Lifecycle Roadmap (CLR), a conceptual framework for establishing and maintaining workforce readiness within an organization. It also describes the readiness test development method, which defines a structured, systematic approach for constructing and piloting readiness tests. Finally, the report illustrates the initial application of the readiness test development method to the role of forensic analyst.

1 Introduction

Workforce effectiveness relies on two critical characteristics: competence and readiness. *Competence* is the sufficient mastery of the knowledge, skills, and abilities—or competencies—needed to perform a given task.[1] *Competence* reflects how well an individual understands subject matter or is able to apply a given skill. Our current research indicates that competence is necessary, but not sufficient, to perform a job task successfully in a real-world work environment. In contrast to competence, *readiness* is the ability to apply a set of competencies required to perform a job task in a real-world environment with acceptable proficiency. In this report, we focus on how to evaluate an individual's readiness to perform his or her job tasks.

Consider the following scenario: A large agency recently hired several people to join its digital analytics team. The new employees' long-term job is to perform forensic evidence collection and digital media analysis both in the field and back at the organization's test lab. As part of their training-and-development activities, the new hires attended several courses that were designed to teach them how to perform key job tasks, including how to use selected forensic tools and how to perform associated analysis tasks.

After the new employees completed the training course for each technique or tool, they were tested to determine if they acquired the competencies needed to use it. The new team members successfully passed all of the individual tests presented to them. After the new team members completed their introductory training courses, the team's leader believed they were ready for field work.

However, when presented with a compromised system to analyze in the field, none of the new team members were able to perform the analysis adequately. More specifically, they were unsure about how to begin the process of investigating the compromised system. The new team members were also unfamiliar with the media involved and unsure about how to collect data from it. Although they could perform parts of the process and use various tools in a classroom setting, these new members of the forensic team failed the test that mattered most—they could not apply what they had learned in the classroom to a real-world work environment. In the end, the new team members were simply not ready to perform their job tasks in the field.

In this example, the new team members demonstrated competence with a suite of techniques and tools in a controlled environment. However, their competence in the classroom did not translate to readiness in the field.

1.1 Background

Several years ago, researchers from the CERT® Division at Carnegie Mellon® University's Software Engineering Institute (SEI) started working with client organizations to improve their train-

[1] For a discussion of competencies, refer to *The People Capability Maturity Model—Guidelines for Improving the Workforce* [Curtis 2002] and the *Project Manager Competency Development Framework* [PMI 2002].

® CERT and Carnegie Mellon are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

ing and development programs. Several of these engagements focused on identifying and documenting cybersecurity competencies.

Competency development is not unique to the SEI. Organizations throughout the community have undertaken similar efforts to develop and document lists of competencies. For example, both the U.S. Office of Personnel Management (OPM) and the National Initiative for Cybersecurity Education (NICE) have developed and documented competency frameworks for the cybersecurity community [OPM 2011, NICE 2011]. The OPM has also developed and documented a Leadership Competency Framework that focuses on an organization's management and leadership roles [OPM 2006]. As a result, we decided to shift our work away from competency documentation and instead address the broader issue of workforce readiness.

In 2011, the CERT Division's CSIRT Development and Training (CDT) team chartered a project focused on building readiness within an organization's workforce. As our team shifted the direction of our research to building workforce readiness, we incorporated previous SEI work in building readiness using certification programs [Behrens 2004] and cybersecurity workforce development [Hammerstein 2010]. In addition, we leveraged the vast body of knowledge in the cognition and performance disciplines pioneered at Carnegie Mellon University, including research into the nature of expertise [Simon, 1996]. We also looked at relevant research throughout the training-and-development community. In particular, we reviewed materials focused on building competency-based training programs, evaluation and assessment methods, and methods for developing effective training and development programs. The bibliography of this report lists these materials.

In 2012, we published a technical note that introduced the Competency Lifecycle Roadmap (CLR), a conceptual framework for developing and maintaining workforce readiness over time [Behrens 2012]. Readiness testing is a major focus of the CLR. After publishing the CLR technical note, we turned our attention toward developing tests designed to assess an individual's readiness to perform job tasks in a real-world environment. This report documents our research results related to readiness testing.

1.2 About this Report

The primary audience for this report consists of managers, training officers, curriculum developers, and course developers who want to improve their organization's training-and-development programs. Researchers focusing on training-and-education activities will also find this document useful. This report also benefits individuals or small working groups who are trying to improve their readiness to perform work tasks.

In general, people who are interested in the following topics will find this report worthwhile:

- developing and maintaining workforce readiness over time
- defining and developing competencies
- developing and administering readiness tests
- understanding personal (or team) goals for competency development and readiness improvement

This report provides a conceptual framework for developing and maintaining workforce readiness over time (i.e., the CLR), documents guidelines for conducting our readiness test development method, and highlights lessons that we learned from administering readiness tests to novice-to-intermediate level forensic analysts. This document comprises the following sections:

- *Section 1: Introduction*—This section presents an overview of workforce competencies, readiness concepts, and the CLR, along with background information on the project.
- *Section 2: Competency Lifecycle Roadmap (CLR)*—This section describes the five activities and two foundational elements of the CLR.
- *Section 3: Overview of the Readiness Test Development Method*—This section provides a broad overview of the steps performed when conducting the readiness test development method.
- *Section 4: Collect Readiness Data (Part 1)*—This section presents guidelines for collecting the data needed to develop a readiness test.
- *Section 5: Develop Readiness Scenarios and Tests (Part 2)*—This section presents guidelines for creating readiness scenarios and tests based on data collected during Part 1 of the method.
- *Section 6: Readiness Testing Pilot Results*—This section describes lessons that we learned from administering readiness tests to novice-to-intermediate level forensic analysts.
- *Section 7: Summary and Next Steps*—This section presents next steps in the development and transition of the CLR and the readiness test development method.
- *Bibliography*—This section lists related publications used to support our readiness research.

The main purpose of this report is to present the method that we developed for creating readiness tests. However, before we dive into the details of the method, we first provide the conceptual basis of our research. The next section of this report describes the CLR, which is the conceptual framework we are using to guide our readiness research.

2 Competency Lifecycle Roadmap (CLR)[2]

Competencies are observable and measurable patterns of knowledge, skills, abilities, behaviors, and other characteristics that an individual needs to perform work roles[3] or occupational functions successfully. Competencies can be decomposed into two types: technical and core competencies. *Technical competencies* apply specifically to a role or position; they directly affect a person's ability to perform a job task.[4] For example, budget planning is a technical competency for a project manager. For a forensic analyst, digital forensics[5] and investigation[6] are important technical competencies.

Core competencies (e.g., communication, teamwork) are cross-cutting and applicable to all occupations and roles within an organization. Core competencies are relevant and important to all individuals, regardless of their technical specialty. Communication is an example of a core competency for both project managers and forensic analysts. The project manager needs to communicate with his or her team when preparing and implementing the project's schedule of events. Likewise, the forensic analyst needs to communicate information about a compromised computer to law enforcement officers.

Behavioral indicators are examples of actions or activities that describe how competencies manifest in observable on-the-job behaviors for specific proficiency levels. Behavioral indicators define specific proficiency levels within a competency. Behavioral-indicator statements convey increased responsibility, scope depth, and complexity for higher proficiency levels. Collecting volatile data from computers (e.g., data in system registers, cache, RAM) is a behavioral indicator of the digital forensics competency (a technical competency for a forensic analyst). Similarly, documenting information about a digital investigation is a behavioral indicator of the communication competency (a core competency for a forensic analyst). Behavioral indicators are important because they provide a means of evaluating an individual's competencies and providing a benchmark of workforce readiness across an organization.

Readiness is the ability to apply the total set of competencies (technical and core) required to perform a job task in a real-world environment with acceptable proficiency. Most job tasks require an individual to synthesize information about multiple subjects and apply multiple skills simultaneously. Readiness is focused on the ability to apply a set of technical and core competencies to complete a job task. Our current research and development activities focus on building workforce

[2] Much of the information in this section was previously published in the conference paper *Affective Strategies for Effective Learning* [Behrens 2012].

[3] A *role* is defined as the duties and responsibilities that make up the work performed by an individual (e.g., forensic analyst).

[4] A *task* is defined as an activity to be performed by the role (e.g., collect data in a forensically sound manner).

[5] *Digital forensics* is defined as collecting, processing, preserving, analyzing, and presenting computer-related evidence in support of network vulnerability mitigation and/or criminal, fraud, and counterintelligence or law enforcement investigations.

[6] *Investigation* is defined as applying tactics, techniques, and procedures for a full range of investigative tools and processes, including (but not limited to) interview and interrogation techniques, surveillance, counter-surveillance, and surveillance detection. Investigation appropriately balances the benefits of prosecution versus intelligence gathering.

readiness in organizations. The conceptual foundation for workforce readiness is the CERT Competency Lifecycle Roadmap (CLR), which is depicted in Figure 1.

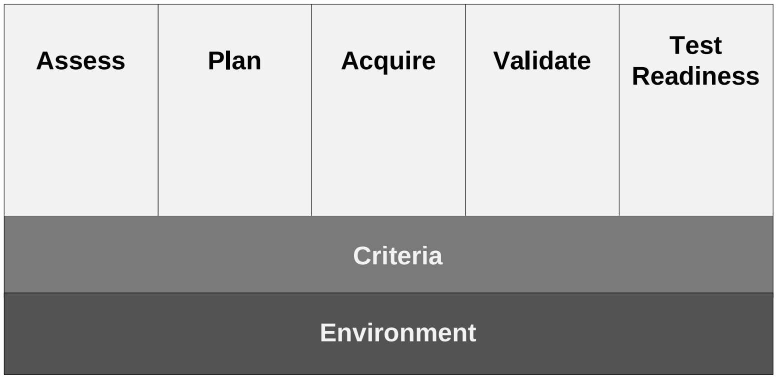

Figure 1: Competency Lifecycle Roadmap (CLR)—Structure

The CLR comprises five core activities—assess, plan, acquire, validate, and test readiness—and two foundational elements that support the activities—criteria and environment. The remainder of this section provides a conceptual overview of each roadmap activity and foundational element.

2.1 Activities

A roadmap *activity* is defined as an action or function that is performed to achieve a specific training and development outcome. The collection of activities in the roadmap is designed to enable an individual to perform a job task in a real-world environment with acceptable proficiency. We begin our discussion of roadmap activities by focusing on the initial assessment of an individual's competencies.

2.1.1 Assess

The first activity, *assess*, is an initial evaluation of key competencies and the ability to perform those competencies in a specific job task. This activity should not be confused with a training assessment, which evaluates the extent to which a training course meets its objectives. In contrast, the roadmap's assessment is a performance-based test that includes measurement of an individual's current competencies. It evaluates an individual's ability to apply a stated competency, regardless of how that competency is acquired (e.g., coursework, experience, or observation). Because knowledge can be broad or specific, gradually or discretely acquired, relevant for long or short periods, or retained or lost over time, a baseline assessment of an individual's current competencies is essential.

Assessment is important to the roadmap because this activity defines a systematic, objective, and repeatable process for establishing a baseline of strengths and weaknesses in the specific competencies needed to perform a specific job task. Assessment also provides insight into which competencies need to be maintained or improved to achieve the desired performance. Competencies that an individual must maintain or improve are called *identified competencies* in this report.[7] In addi-

[7] The identified competencies constitute the subset of all key competencies that must be addressed by an individual.

tion, as an organization assesses groupings of competencies, it gains an overall picture of an individual's relative strengths and weaknesses, which can assist that individual with professional growth opportunities. Table 1 presents the key characteristics of the *assess* activity.

Table 1: Characteristics of the Assess Activity

Dimension	Description
What	• an initial evaluation of key competencies and the ability to perform them in a specific job task
Why	• to identify a baseline of strengths and weaknesses in the key competencies needed to perform a specific job task • to apply a systematic, objective, and repeatable process • to provide insight into how to maintain or improve the performance of identified competencies

Multiple types of assessments can be used to evaluate an individual's competencies. Each organization needs to determine what works best in its environment. Examples of methods that might be used to assess an individual's competencies include

- Conduct a performance-based test that includes measurement of the current state of key competencies.
- Have individuals complete a skills inventory with supporting substantiation showing evidence that they mastered those skills. Examples of evidence include course certificates and the results of a manager's evaluation.

2.1.2 Plan

The next roadmap activity, *plan*, defines an individual's intended course of action for maintaining or improving specific competencies that are needed to perform a specific job task. Table 2 presents the key characteristics of the *plan* activity.

Table 2: Characteristics of the Plan Activity

Dimension	Description
What	• a course of action intended to maintain or improve identified competencies
Why	• to specify an attainable path for maintaining or improving identified competencies • to communicate the path for maintaining or improving identified competencies

The *plan* activity is important because it specifies an attainable path that an individual can follow to maintain or improve identified competencies. Here, an individual determines which options and resources are available and relevant. Once the path, or development plan, has been developed, the individual documents it and then disseminates it to all relevant stakeholders. Planning thus lays the foundation for acquiring identified competencies, which is the next roadmap activity.

Some examples of planning methods include the following:

- Map strengths and weaknesses to options and resources provided within the organization and community to develop a path for maintaining or improving identified competencies. This mapping may often take the form of an individual development plan (IDP).
- Document and disseminate the path for maintaining or improving identified competencies.

2.1.3 Acquire

The *acquire* activity of the roadmap defines actions that are taken to maintain or improve identified competencies.[8] Acquisition of competencies is important because it enables an individual to reinforce strengths and address weaknesses in his or her competencies. Table 3 presents the key characteristics of the *acquire* activity.

Table 3: Characteristics of the Acquire Activity

Dimension	Description
What	• actions taken to maintain or improve identified competencies
Why	• to reinforce strengths and address weaknesses in the ability to perform a specific job task

Depending on a task's complexity and requirements, multiple modalities can be used to maintain or improve competencies, including one or more of the following:

- a training course or curriculum
- mentoring or other on-the-job training opportunities, such as ride-alongs
- shadowing management or other subject matter experts
- a realistic simulation environment
- targeted self-study (e.g., technical journals, online discussions, or topical blogs)
- conference attendance and participation
- academic coursework or degree programs

2.1.4 Validate

Validate is the roadmap activity that measures whether an individual's training-and-development actions have addressed his or her competency needs. Validation of acquired competencies is achieved by conducting a performance-based test to determine if an individual has maintained or improved identified competencies through his or her actions. It defines a structured approach to measuring the competencies that were acquired successfully. Table 4 presents the key characteristics for the *validate* activity.

Table 4: Characteristics of the Validate Activity

Dimension	Description
What	• a measure of whether actions have addressed identified competencies
Why	• to ensure that identified competencies have been adequately maintained or improved

Validation methods can include

- quizzes
- certification exams
- targeted interviews (by experts)
- performance in a classroom exercise or simulation
- observation of an employee demonstrating what was learned

[8] For further discussion of competencies and training, refer to the *Handbook for Developing Competency-Based Training Programs* [Blank 1982].

Validation focuses on the competencies that an individual has acquired through participation in training-and-development actions (e.g., training, academic course, class, conference attendance, on-the-job training). Its emphasis on measuring the extent to which competencies have been acquired differs from that of the next roadmap activity, *test readiness*, which evaluates the application of competencies in an actual work environment.

2.1.5 Test Readiness

Often overlooked or grouped with validation, the *test readiness* activity of the roadmap is a real-world evaluation of whether a person can perform a specific job task as required. People bring a range of knowledge and experiences to any job setting or task. The initial assessment and subsequent validation determines an individual's knowledge of and experience with certain competencies and his or her understanding of some targeted (often highly technical or organization-specific) competencies.

However, knowing an individual's current proficiency in selected competencies is insufficient for predicting that individual's overall readiness to perform a given job task. An individual might be able to apply certain competencies in a controlled environment, but might not be able to apply them in a real-world setting. The ability to test an individual's readiness to perform a job task is an essential component of an effective training and development program. Table 5 presents the key characteristics of testing an individual's readiness to perform assigned tasks.

Table 5: Characteristics of the Test Readiness Activity

Dimension	Description
What	• a real-world evaluation of whether a specific job task can be performed as required
Why	• to ensure that competencies can be appropriately applied to job tasks

Approaches for assessing readiness can include

- real-world scenarios
- role-playing exercises
- capstone exercises
- real-world simulations
- observation of real-world task performance

Readiness tests are derived from the requirements needed to complete a given job task in its real-world context. Rather than assessing competencies in isolation, a readiness test assesses an individual's ability to apply a group of technical and core competencies needed to perform and excel at that job task. We describe readiness tests in greater detail in Sections 3-6 of this report.

2.2 Foundational Elements

The CLR defines a *foundational element* as an entity that supports the execution of roadmap activities. The inclusion of foundational elements is one of the most important ways in which the CLR differs from other models and approaches to many training and development programs, whose moderate success in achieving desired outcomes may be due in part to their exclusion of such elements. The two foundational elements of the CLR are *criteria* and *environment*.[9]

[9] The *environment* is sometimes referred to as *context*.

2.2.1 Criteria

Criteria, the first foundational element of the roadmap, are the sets of technical and core competencies and associated behavioral indicators that define the requirements for performing a job task. Criteria define the range of competencies and behavioral indicators needed to establish an individual's readiness to perform a task. Similar to the conclusions of other research-and-development efforts related to training and competency-based programs, our research indicates that competencies are contextual in nature. Competencies work best when they are aligned with a role and, in particular, when they are described in terms of the work that is actually done. Table 6 defines the characteristics for the *criteria* element of the roadmap.

Table 6: Characteristics of the Criteria Element

Dimension	Description
What	• sets of technical and core competencies that define the requirements for performing assigned tasks
Why	• to establish the scope of performance requirements that define readiness

The scope of CLR criteria is more granular than it might appear at first glance. Criteria must be understood clearly, both in depth and breadth, for a given job task. And, perhaps most importantly, criteria must support each CLR activity in such a way that an individual's growth in knowledge and performance can be measured in a variety of ways over time.

The CLR can be applied across many disciplines, in part because it can incorporate multiple sets of criteria, such as those from the

- National Initiative for Cybersecurity Education (NICE) cybersecurity competencies [NICE 2011]
- OPM Leadership Competency Framework [OPM 2006]
- OPM Competency Model for Cybersecurity [OPM 2011]
- Project management competencies from the Project Management Institute [PMI 2002]

2.2.2 Environment

The second foundational element of the roadmap is the *environment*, which includes the people, processes, culture, and context that influence the execution of roadmap activities. In some instances, conditions within the environment facilitate or enable the successful completion of roadmap activities. In other instances, conditions hinder the execution of roadmap activities, acting as barriers to a successful training and development program.

The roadmap's environment element gives users the structure and support they need to work in a dynamic organizational setting. The environment is important because it ensures a strong relationship between the training and development program and people's readiness to perform their assigned tasks. Table 7 presents the key characteristics for the training and development program's environment.

Table 7: Characteristics of the Environment Element

Dimension	Description
What	• processes, culture, and context that influence the execution of the competency lifecycle activities
Why	• to provide the structure and support needed to work in a dynamic organizational setting • to ensure a strong relationship between training and development goals and readiness to perform assigned tasks

Key environmental factors in the success of a training and development program can include

- a designated training coordinator to ensure the training program is institutionalized, updated, and socialized
- clear policies and processes that detail staff and management requirements for training and development
- outlined, streamlined processes for achieving training goals
- time for management to meet with each employee to discuss career and professional development and to perform a yearly assessment of the needed competencies for performing job functions satisfactorily
- time for staff to pursue training and development activities, even addressing training as a work assignment
- a centralized tracking system to allow management and staff to track training plans and accomplishments
- a culture of training and education within the organization that recognizes the importance of developing and sustaining competencies and that encourages such pursuits through verbal communication and dedication of time and resources
- recognition by staff and management that training and development is more than just completing yearly compliance modules for ethics, security, privacy, and other such practices

2.3 Roadmap Implementation Over Time

The roadmap can be used to define an individual’s training development path over time. Figure 2 illustrates this process, in which the roadmap establishes an individual’s progression from novice to expert for a given job task.

Each level of job proficiency (novice, intermediate, and expert) has a unique set of criteria (competencies and behavioral indicators) that define the requirements for performing assigned tasks at that level. The environment affects all levels of job proficiency and either facilitates or hinders an individual’s progression over time. In addition, the core roadmap activities (assess, plan, acquire, validate, and test readiness) are performed continuously throughout this progression. The progression across levels of expertise defines an individual’s training and development path within an organization, providing a roadmap for improving an individual’s competencies.

This roadmap is not intended to be used in a linear fashion. All people have some areas of expertise, some areas that need to be developed, and perhaps some areas that are outside an individual’s interest or ability. The notion of readiness may be iterative and certainly accounts for criteria at all levels, from novice to expert. While time is an important factor, it is only one indicator of the growth of competency-based readiness. Other indicators might include experience or collective abilities of a work team.

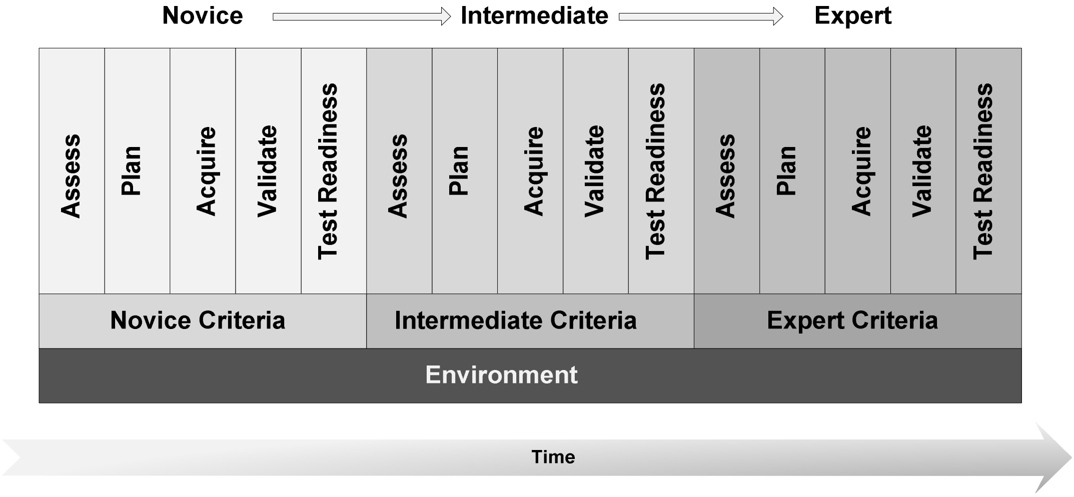

Figure 2: Competency Lifecycle Roadmap (CLR)—Progression Over Time

Overall, we envision that organizations will apply the CLR concept in many ways, including

- identifying gaps in their training and development program by benchmarking it against the CLR
- helping them improve their training and development program
- providing guidance for developing a curriculum or training plan
- helping an individual set personal goals related to a specific job or task assignment

While the CLR has many potential uses, we originally designed it as a conceptual framework for developing and maintaining workforce readiness over time. As a result, we used the CLR as the touchstone for our research into assessing workforce readiness. In the next section, we shift the focus of this report from the concepts of the CLR to a tangible method that we developed for creating readiness tests.

3 Overview of the Readiness Test Development Method

A readiness test is a real-world evaluation of whether a person can perform a specific job task as required. Rather than evaluating individual competencies in isolation, a readiness test assesses an individual's ability to apply a group of technical and core competencies needed to perform and excel at a job task. These tests are derived from scenarios that describe how to complete a given job task in its real-world context.

In this section, we provide an overview of the scenario-based method that we developed to construct test readiness. The readiness test development method is divided into two parts:

- Part 1: Collect Readiness Data
- Part 2: Develop Readiness Scenarios and Tests

Part 1 of the method is focused on data collection. Here, the goal is to collect data from subject matter experts (SMEs) about what constitutes readiness for specific job tasks. These data provide the basis for test development, which is the goal of Part 2. Table 8 provides a summary of the steps that are performed during each part of the method.

Table 8: The Readiness Test Development Method

Part	Step	Step Description
Part 1: Collect Readiness Data	1.1 Characterize the Role Being Analyzed	Step 1.1 establishes a broad understanding of the role and its basic responsibilities. Information from this step provides a foundation for the remaining steps in Part 1.
	1.2 Identify Important Job Tasks	This step elicits the range of job tasks that must be performed by the given role.
	1.3 Select a Job Task to Analyze in Detail	During Step 1.3, the focus shifts from gathering broad information about a role to gathering detailed information about one of the tasks performed by that role.
	1.4 Analyze the Selected Job Task	Step 1.4 begins the deep dive into one of the role's important job tasks. The goal of this step is to analyze how the selected task is performed.
	1.5 Identify Barriers for the Selected Job Task	Step 1.5 requires the collection of data about circumstances that prevent people from performing a job task satisfactorily (called stresses).
	1.6 Identify KSAs[10] for the Selected Job Task	This step establishes which KSAs are required to complete the selected job task.
Part 2: Develop Readiness Scenarios and Tests	2.1 Develop Readiness Scenarios	Step 2.1 kicks off the process of developing readiness tests. The goal of this initial step is to develop scenarios that describe job tasks in a real-world work environment.
	2.2 Validate Readiness Scenarios	Each readiness scenario developed during Step 2.1 is based on data collected during Part 1. In Step 2.2, SMEs review the scenarios to ensure that each scenario is realistic, correct, and complete.
	2.3 Design and Develop Readiness Tests	This step transforms the readiness scenarios into readiness tests.

[10] KSAs are knowledge, skills, and abilities.

Part	Step	Step Description
	2.4 Evaluate Readiness Tests	The final step in the method requires each readiness test to be piloted with participants from the intended audience. The goal is to evaluate the effectiveness of each test and make improvements and adjustments as needed

We applied the steps outlined in Table 8 to develop readiness tests for the role of a forensic analyst. In the next two sections, we provide guidelines for performing each step of the readiness test development method and describe the results from our initial application of the method. We start in the next section by describing the data-collection steps performed during Part 1 of the readiness test development method.

4 Collect Readiness Data (Part 1)

The goal of Part 1 is to collect data about what constitutes readiness for a given role. These data are elicited from SMEs who have knowledge and insights about the job tasks that must be performed by the role.[11] To elicit these data, we conduct interviews with the SMEs. At a minimum, we include the following people in each interview session:

- *Lead interviewer*—This person is responsible for leading the interview session. The lead interviewer provides SMEs with context about the session (e.g., purpose of the session, summary of session activities). The lead interviewer facilitates all discussions during the interview and also takes notes as needed during the session.
- *Interview team members*—These people are responsible for taking notes during the session and asking follow-up questions. Team members might also assume additional responsibilities as required, such as keeping time during the session.
- *SMEs*—These people are responsible for providing information about the job tasks that must be performed by a role. SMEs have knowledge and insights about the selected role that are elicited and recorded (i.e., note taking) during the interview session. An interview session typically includes one to three SMEs.

The focus of our initial application of the method was *forensic analysis* (also called digital media analysis). In particular, we were interested in gathering information about high-priority job tasks performed by novice-to-intermediate level forensic analysts (our audience for readiness testing). Two SMEs with considerable field experience as forensic analysts were interviewed by our team. We interviewed each SME separately. Table 9 illustrates our interview schedule for each SME.

Table 9: The SME Interview Schedule

Session	Description	Time
Session 1	The first interview session focused on gathering broad information about the given role (e.g., job description, position in organizational hierarchy, high-priority tasks). The following steps were completed during Session 1: • Characterize the Role Being Analyzed (Step 1.1) • Identify Important Job Tasks (Step 1.2) • Select a Job Task to Analyze in Detail (Step 1.3)	90 minutes
Session 2	The second session focused on gathering in-depth information about a specific job task.[12] The following steps were completed during Session 2: • Analyze the Selected Job Task (Step 1.4) • Identify Barriers for the Selected Job Task (Step 1.5) • Identify KSAs for the Selected Job Task (Step 1.6)	90 minutes

[11] The data required to develop readiness scenarios can be collected using multiple methods, such as job task analysis and ethnographic study. The guidelines provided in this section are based on a job task analysis.

[12] During the pilot, we gathered information about only one high-priority job task during Session 2. If we decided to gather in-depth information about other job tasks, we would have added an additional interview session for each additional job task.

In the remainder of this section, we briefly describe each step performed during Part 1 of our method for developing readiness tests. For each step, we present the guidelines we follow when conducting that step as well as the results for our initial application of the method (i.e., for forensic analysis). We begin with Step 1.1, *Characterize the Role Being Analyzed.*

4.1 Characterize the Role Being Analyzed (Step 1.1)

Step 1.1 kicks off the interview process for readiness testing. The goal of this initial step is to establish a broad understanding of the role and its basic responsibilities. The information gathered during this step provides a foundation for all subsequent interview questions.

4.1.1 Guidelines

The interviewer asks the SMEs about the basic responsibilities of their role. This information is vital to understanding the range of tasks that must be performed by the individual who is fulfilling the selected role. To gather this information, the interviewer asks the SMEs the following types of questions:

- What is the basic job description for this role?
- Where does this role fit into the organization?
- To whom do the people in this role report?
- With whom do people in this role interact? With whom must they communicate? With whom must they share information?

Once the interview team establishes a broad understanding of the given role, it is ready to collect more detailed information about the role.

4.1.2 Results

We learned that a digital investigation has two core goals: (1) to collect data from designated information technology equipment and (2) to analyze the collected data. The two goals are typically addressed by different people and require different skill sets. When collecting data, investigators visit the place(s) where the data "live," such as an office, home, or information technology (IT) department. The purpose of data collection is to gather images of disks, file servers, etc., from a site and bring those images back to the forensic organization for analysis.

At the forensic organization, the images are then copied onto an analysis platform for detailed examination. Forensic analysts look for evidence that supports the investigation being conducted. They either find evidence that supports the legal case being developed or not (i.e., find exculpatory evidence). After their work is complete, the analysts document their findings (e.g., what was found and where it was found). These findings form the basis for their report. However, the job of an analyst does not end with the report. He or she might have to testify about the findings during formal court proceedings.

4.2 Identify Important Job Tasks (Step 1.2)

Each role within an organization is normally required to perform multiple job tasks. Our readiness testing approach evaluates an individual's readiness to perform selected, high-priority job tasks for his or her assigned role. During Step 1.2, we elicit a range of job tasks that must be performed by the given role.

4.2.1 Guidelines

During Step 1.2, the lead interviewer asks SMEs to consider the following questions:

- What are your important job tasks?
- What are the expectations for your job?
- What goals are you trying to accomplish in this job?
- What are your hardest tasks?
- Tell me about a typical day on the job. What do you do?
- Do you perform any tasks that are not particularly important to your job? What are they?

The SMEs brainstorm the important job tasks performed by the role, interview team members, and record the ideas generated by the SMEs. At the conclusion of Step 1.2, the interview team has a documented list of job tasks performed by the SMEs.

4.2.2 Results

During our interview sessions with forensic SMEs, they identified the following job tasks as being integral to the role of forensic analyst:

- *Prepare*—Preparation involves having the right equipment for gathering data at a site.
- *Identify data*—Based on the event being investigated, the forensic analyst performs reconnaissance to identify which technologies are deployed at a site and determine which data need to be collected from the organization’s systems and networks.
- *Collect data*—The forensic analyst gathers identified data from an organization’s systems and networks.
- *Analyze data*—Data that are collected are interpreted to yield insights that are relevant to the event being investigated.
- *Write a report*—The results of the digital investigation are documented in a report. The purpose is to describe the timeline for the event.

These five tasks provide a range of activities typically performed by forensic analysts. Next, we select one of those tasks to examine in greater detail.

4.3 Select a Job Task to Analyze in Detail (Step 1.3)

Readiness tests are developed for high-priority job tasks that must be performed by the given role. Up to this point, the interview is focused on understanding the breadth of tasks performed by the role. Here, the focus shifts from gathering broad information about a role to gathering detailed information about one of the tasks performed by that role.

4.3.1 Guidelines

In Step 1.3, the interview team and SMEs decide which task to analyze in detail. The interviewer asks the following types of questions:

- Which of your job tasks are most important? Why?
- Which job tasks would you like to examine in more detail? Why?

When selecting a job task, the interview team and SMEs should consider tasks that are appropriate for the audience to be tested. The experience and skill level of the people who are taking the test are a key factor in selecting a task. The team and SMEs should also look for a job task that

- is big or complex
- has a number of interfaces
- requires core competencies (e.g., communication, teamwork)
- requires more than one set of competencies
- is procedural in nature
- produces a clear output

After the task is selected, the interview team and SMEs are ready to conduct a deep dive into that job task.

4.3.2 Results

The SMEs suggested *data collection* as the job task to examine further. Data collection is typically performed by junior members of a forensic team, which is the target audience for our readiness tests. As a result, we agreed with the SMEs suggestion and turned our attention to collecting detailed information about forensic data collection.

4.4 Analyze the Selected Job Task (Step 1.4)

Step 1.4 begins the deep dive into one of the role's important job tasks. The goal of this step is to analyze how the selected task is performed. The information gathered during this step establishes the scope of the selected job task.

4.4.1 Guidelines

The interviewer asks the SMEs the following types of questions:

- How do you perform this job task?
  - What activities do you perform?
  - When do you perform those activities?
  - Who else works on these activities with you? What do they do?
- What decisions do you have to make when performing this task? Which decisions are most important?
- What are the boundaries of this job task? What don't you need to do when completing this task?
- How do you know when you have completed this task?

At this point, the interview team has established how to perform the selected task. This information provides the basis for developing readiness tests.

4.4.2 Results

The SMEs discussed how they collect data in a forensically sound manner. During data collection, an investigator (i.e., forensic analyst) typically completes the following activities:

- asks questions of site personnel to gather additional information relevant to data collection (e.g., where files of interest are located, types of applications running on the hard drive, whether encryption is being used)
- copies volatile memory from the computer’s random access memory (RAM)
- images the hard drive in a forensically sound manner
- takes careful notes during data collection (e.g., notes about the equipment and how it was configured, which actions were taken and when)
- prepares drives for transport back to the lab for analysis

The analysis performed during Step 1.4 defines how investigators collect data in a forensically sound manner. However, a task analysis is only one aspect of characterizing job performance. A second aspect is defining any barriers that can interfere with job performance. Eliciting such barriers is the focus of Step 1.5.

4.5 Identify Barriers for the Selected Job Task (Step 1.5)

During Step 1.5, the interview team collects data about circumstances that prevent people from performing a job task satisfactorily. These problematic circumstances are also called *stresses*. Information about stresses are used to develop readiness tests that evaluate an individual’s ability to navigate through problems that commonly occur in the real-world work environment. These “stress scenarios” are used to evaluate different levels of proficiency (novice, intermediate, expert) related to a job task.

4.5.1 Guidelines

The goal of this step is to document a list of barriers for the selected job task. The interviewer begins the discussion by asking the following questions:

- What gets in your way when you perform this job task? How do you get around these barriers?

  Consider:

  - People, process, and tool barriers
  - Knowledge barriers
  - Other barriers
- Whose help do you need to perform the task? How do you know? How do you get that help?

Barriers define real-world circumstances that influence whether a task is completed correctly and completely. Barriers are essential for ensuring that readiness testing accurately reflects the work environment in which a job task is performed.

4.5.2 Results

The SMEs discussed a range of barriers. The following list provides a few examples of barriers (i.e., stresses) identified by the SMEs:

- Incorrect information about the computer's configuration is provided by site personnel.
- RAID (redundant array of independent disks) is implemented in the computer of interest.
- The computer might have a different operating system than anticipated.
- The computer is locked and encrypted, and site personnel will not help.
- The site being investigated employs novel technology with which the data collector is not familiar.
- The site's information-technology staff is not helpful. They will not provide the data collector with administrative access to the computer.
- The data are not physically located at the site (e.g., data are stored in the cloud).

At this point, we have analyzed the selected job task (Step 1.4) and identified several barriers/stresses that can prevent completion of the task (Step 1.5). Next, we turn our attention to specific KSAs that are needed to complete the task.

4.6 Identify KSAs for the Selected Job Task (Step 1.6)

Readiness is the ability to apply the total set of competencies (technical and core) required to perform a job task in a real-world environment with an acceptable proficiency. To complete their job tasks, individuals synthesize information about multiple subjects and apply multiple skills simultaneously. During Step 1.6, the interview team establishes which KSAs are required to complete the selected job task.

4.6.1 Guidelines

The interviewer asks the SMEs the following questions:

- What KSAs do you need to perform this job task?
  - *Technical Competencies*: Which KSAs directly contribute to the completion of the task? How?
  - *Core Competencies*: Which KSAs enable or support the completion of the task? How?
- What other KSAs do you envision people needing for this job task in the future?

At the conclusion of this step, the interview team has a list of KSAs related to the selected job task. At this point, the majority of the data needed to construct readiness tests has been collected.

4.6.2 Results

The SMEs identified the following technical KSAs for forensic data collection:

- knowledge of system administration concepts
- knowledge of hard drives and file systems (e.g., how data are written to drives)
- knowledge of chain-of-custody practices (e.g., knowing the sign-off procedures for data)

- knowledge of data-collection practices for digital investigations
- knowledge of evidential procedures (e.g., do not boot the hard drive if you don’t have to)
- ability to image a hard drive
- ability to collect volatile data (e.g., data in system registers, cache, RAM)
- ability to use imaging tools (e.g., dd, dc3dd, FTK imager, EnCase acquisition)
- ability to use hash values (e.g., MD5)

In addition, the experts indicated that the following KSAs support an individual’s ability to collect data in a forensically sound manner:

- knowledge of the business and mission of the organization being investigated (e.g., organizational structure, knowing who is responsible for what)
- ability to solve problems
- ability to document information and keep good records
- ability to use support tools when documenting information
- ability to communicate with team members (including the team leader)
- ability to communicate with onsite stakeholders (e.g., IT staff, management)
- ability to gather information about a situation by asking effective questions

At the conclusion of Part 1, we had gathered considerable data related to forensic data collection, including

- description of a role (forensic analyst) and where it fits into the organizational structure
- important job tasks performed by a forensic analyst
- a job task performed by forensic analysts to examine in more detail (forensic data collection)
- analysis of how forensic data collection is performed
- a list of barriers (i.e., stresses) that can prevent people from collecting data in a forensically sound manner
- technical and core KSAs needed to perform forensic data collection

We use these data during Part 2 of the method when we develop readiness scenarios and tests. The next section of this report provides a detailed discussion of how we develop and validate readiness scenarios and tests.

5 Develop Readiness Scenarios and Tests (Part 2)

During Part 2 of the method, the development team creates readiness tests for job tasks selected during Part 1. The contributors during Part 2 of the readiness test development method include

- *Development Team*—This team is responsible for designing, building, and evaluating readiness tests. The development team includes the people who collected data from SMEs during Part 1. The development team can be expanded to include individuals with specialized expertise, such as instructional designers and technical experts.
- *SMEs*—These people are responsible for providing feedback about readiness scenarios. SMEs have knowledge and insights about the job tasks that have been selected for readiness testing. SMEs participating in Part 2 activities are normally the same experts who took part in Part 1 interview sessions.
- *Test Administrator*—This person (or people) administers readiness tests to participants when piloting the readiness tests.
- *Participants*—These people take the readiness tests during pilots.

We explored the role of forensic analyst (also called digital media analyst) in our initial application of the readiness test development method. We decided during Part 1 of the method to develop readiness tests for forensic data collection, a high-priority job task performed by forensic analysts. In the remainder of this section, we briefly describe each step performed during Part 2 of the method. For each step, we present guidelines for completing that step as well as the pilot results for forensic data collection. We begin with Step 2.1, *Develop Readiness Scenarios*.

5.1 Develop Readiness Scenarios (Step 2.1)

Step 2.1 kicks off the process of developing readiness tests. The goal of this initial step is to develop readiness scenarios that describe job tasks in a real-world work environment.[13] These scenarios provide the basic requirements for the associated readiness tests to be designed and developed (in Step 2.3).

5.1.1 Guidelines

Development team members review the data collected during the SME interviews and consider the following questions:

- What job task is being evaluated?
- What occurs in the basic scenario?
- Which stresses or barriers will be evaluated?

[13] A readiness scenario describes how a job task is performed in a real-world work environment. The scenario describes a job task that an individual must complete, outlines what the individual must accomplish during the scenario, highlights how other roles interact with the individual during the completion of the job task, describes any barriers that the individual must overcome, and presents the technical and core competencies that the individual needs for the scenario. A readiness scenario is narrowly focused on how an individual performs a single job task. This narrow scope enables us to develop objective grading criteria for the corresponding readiness test.

- Which technical competencies are relevant to the basic scenario? Which are relevant to each stress scenario?
- Which core competencies are relevant to the basic scenario? Which are relevant to each stress scenario?
- What tests will be used to evaluate the basic scenario (e.g., simulation, classroom exercise, oral exam, knowledge test)? What tests will be used to evaluate each stress scenario?
- Which behavioral indicators[14] are evaluated by each test?

Development team members use the above questions to guide the process of developing readiness scenarios.

5.1.2 Results

We developed a readiness scenario for forensic data collection. The readiness scenario describes an investigation into malicious cyber activity originating within a large government civilian agency. In the scenario, a team from a government unit is assigned to investigate the malicious activity. An investigator from the team travels to the government agency's site to collect data from an affected computer. During the data-collection activity, the investigator performs the following basic tasks:

- asks questions of site personnel to gather additional information relevant to data collection (e.g., where files of interest are located, types of applications running on the hard drive, whether encryption is being used)
- copies volatile memory from the computer's random access memory (RAM)
- images the hard drive in a forensically sound manner
- takes careful notes during data collection (e.g., notes about the equipment and how it was configured, which actions were taken and when)
- prepares drives for transport back to the lab for analysis

The complete scenario for forensic data collection is provided in Appendix A. The scenario in Appendix A is the basic readiness scenario; it does not include any stresses or barriers that a forensic analyst would have to overcome to collect data in a forensically sound manner.

We also developed one stress scenario. After considering the range of stresses identified during our interviews with the SMEs in forensic analysis, we selected the following stress to include in a scenario: *RAID (redundant array of independent disks) is implemented in the computer of interest*. The complete stress scenario is found in Appendix B.

5.2 Validate Readiness Scenarios (Step 2.2)

Each readiness scenario developed during Step 2.1 is based on the development team's understanding of the data it collected during previous data-collection interviews with SMEs (during Part 1). In Step 2.2, the development team engages the SMEs to ensure that the scenarios are realistic, correct, and complete.

[14] Behavioral indicators are derived from the KSAs elicited during Step 1.6, *Identify KSAs for the Selected Job Task*. Refer to Section 4.6 for more information about Step 1.6 of the readiness test development method.

5.2.1 Guidelines

Development team members and the SMEs review each scenario and consider the following questions:

- Does each scenario accurately reflect the job task? Why or why not?
- Which aspects of each scenario work well? Why?
- Which aspects of each scenario could be improved? Why?
- Is the basic scenario realistic? What level of expertise (e.g., novice, intermediate, expert) would be required to complete the basic scenario?
- Is each stress scenario realistic? What level of expertise (e.g., novice, intermediate, expert) would be required to complete each stress scenario?

The above questions are used to guide a discussion between the development team and the SMEs. The development team notes where each scenario needs to be adjusted and documents ideas for improving the scenario. Scenario validation can be iterative. For example, the development team might engage the SMEs, make changes to the scenario, and then review the updated scenarios with the SMEs. The goal is to iterate with the SMEs until the scenarios accurately describe job tasks in a real-world work environment.

5.2.2 Results

We reviewed the basic and stress scenarios with the SMEs. They helped us to refine each scenario by correcting minor errors in terminology and by providing additional details where needed to make the scenarios more realistic. The basic and stress readiness scenarios documented in Appendices A and B are the final versions (i.e., after incorporating the SMEs' comments).

5.3 Design and Develop Readiness Tests (Step 2.3)

Step 2.3 transforms the readiness scenarios into readiness tests. Here, the development team designs a readiness test for each scenario that was developed and validated. Once the design of a readiness test is complete, the team then develops the test in accordance with the design.[15]

5.3.1 Guidelines

Readiness scenarios establish requirements for the tests that are designed and developed during this step. When performing Step 2.3, development team members start by reviewing each readiness scenario and considering the following questions:

- What scenario is being evaluated? Which stresses are included in the scenario?
- What type of test (e.g., simulation, classroom exercise, oral exam, knowledge test) is being designed?
- What artifacts (e.g., instructions, answer keys) need to be developed?
- Will technology (e.g., hardware, software) be used to support administration of the test? If yes, what technology will be used? Who will develop the technology?

[15] When developing readiness tests, we applied basic instructional design concepts and principles.

- What occurs during the test?
- What are the success criteria for the test? How will you know if someone passes (or fails) the test?
- Who will develop the readiness test?

The above questions are used to guide the development team as it designs and develops each readiness test.

5.3.2 Results

We decided that the readiness tests for forensic data collection would be role-based simulations of the scenarios. In the tests, participants (i.e., the people taking the test) must collect data from actual hardware that is set up for them. The tests include the following roles:

- *data collector*—The data collector is the person performing the data collection.
- *site personnel*—At least two site roles are specified: (1) an IT staff member and (2) a business operations manager.

In the test designs, we specified that the participant plays the role of data collector. Alternatively, we allowed for the possibility that a team could take the test. Here, multiple participants would work as a team to forensically collect data from the affected computer. Finally, the design specifies that test administrators play the site-personnel roles. Ideally, multiple test administrators assume the site roles. However, a single test administrator can assume all of the site roles when needed. Both the basic and stress scenarios include the same roles. The design for the basic scenario is provided in Appendix C, while the design for the stress scenario is presented in Appendix D.

5.4 Evaluate Readiness Tests (Step 2.4)

The readiness tests produced by Step 2.3 reflect the scenarios developed and validated in Steps 2.1 and 2.2 respectively. In Step 2.4, the development team administers each readiness test to multiple participants and evaluates the results. The goal is to ensure that the test assesses readiness appropriately.

5.4.1 Guidelines

Development team members consider the following questions:

- Which aspects of the readiness test worked well for each participant?
- Which aspects of the readiness test did not work well for each participant?
- What feedback did each participant provide?
- What aspects of the readiness test could be improved?
- Does the underlying scenario need to be changed?
- Are the success criteria correct and complete?

The above questions are used to guide the evaluation of readiness tests. The development team administers each readiness test to the participants. The development team notes where each readiness test needs to be adjusted and documents ideas for improving the test. This evaluation activity can be iterative. For example, the developer might administer the test to a set of participants, make changes to the tests based on the feedback, and then administer the updated tests to another set of participants. The ultimate goal is to develop tests that assess readiness appropriately.

5.4.2 Results

We piloted the readiness tests for forensic data collection (basic and stress versions) with two audiences and used the resulting lesson learned to improve the tests. The next section of this report presents the details of our pilot activities and summarizes the lessons that we learned from conducting the pilots.

6 Readiness Testing Pilot Results

As described in the previous section, the final step in the readiness test development method requires us to pilot each readiness test with the intended audience. The goal is to evaluate the effectiveness of each test and then make improvements and adjustments as needed. This section highlights the following pilot activities that we conducted for the forensic data-collection readiness tests:

- *internal pilot and review activities*—We engaged with technical staff and students from our organization to evaluate the readiness tests.
- *external pilot*—We conducted readiness tests with people who were participating in a government cybersecurity fellowship program (i.e., members of our target audience).

In the remainder of this section, we describe the pilot and review activates that we conducted. We also provide a summary of the key lessons that we learned from piloting readiness tests for forensic data collection.

6.1 Internal Pilot and Review Activities

We engaged with technical personnel from our organization for the first round of pilots. For this initial round of piloting, we selected participants from opposite ends of the experience spectrum: one novice security analyst and one highly experienced security analyst.[16] For our internal piloting and review of the readiness test for forensic data collection, we completed the following activities:

- *Pilot 1*: We conducted a pilot of the basic readiness test for forensic data collection with a novice analyst. Our goal was to evaluate the readiness test with someone from our target audience.
- *Design Review*: We performed a detailed walk-through of the test design based on the lessons learned from the initial pilot.
- *Pilot 2*: We conducted a pilot of the basic readiness test for forensic data collection with an experienced member of the technical staff. Here, our goal was to evaluate the basic readiness test with someone with considerably more experience than our target audience.

During the two pilots, we provided participants with a relatively small number of success criteria and a basic set of instructions. We let each participant decide how to navigate through the available options to complete the test. These internal pilots were conducted without time limits and were generally less structured than external pilots we performed later. In the remainder of this sub-section, we present the highlights of each pilot and review activity, beginning with the pilot with a novice analyst.

[16] While both participants had background and experience in information security, neither was a forensic analyst.

6.1.1 Pilot 1: Novice Analyst

Our target audience is someone who (1) has a degree in a security-related field and (2) has some (although limited) real-world experience.[17] The participant in our first pilot was a graduate student studying information security. For the past year, this participant supported CERT technical staff members on several projects. Overall, this participant reasonably fit the profile of our target audience.

We administered the basic readiness test for forensic data collection to the participant. The test is a role-playing exercise based on a forensic data-collection scenario. In that scenario, a forensic team from a government unit is conducting an investigation into malicious cyber activity originating within a large government civilian agency. The readiness-test participant plays the role of team member who travels to the government agency's site to collect data from an affected computer. The participant is instructed to collect data from hardware that test administrators have set up in a conference room. (For more information on the readiness test administered in this pilot, refer to Appendix A for the readiness scenario and Appendix C for the test design.)

During this pilot, our goals were to evaluate how well the participant understood the instructions for taking the test and gauge the difficulty of the readiness test. The test administrator orally provided a basic set of instructions to the participant that addressed the scenario and the role that the participant was playing. In addition, the participant was provided with a laptop that contained the tools needed to complete the test and reference materials. However, the test administrator did not walk through the laptop and reference materials with the participant.

The participant had difficulty beginning the test. The purpose of the laptop and reference materials had not been explained in sufficient detail. For example, not every tool on the laptop was needed to complete the test and using the reference materials was not required. Here, the vagueness of our instructions regarding the use of laptop and reference materials inadvertently introduced a stressor to our basic readiness test (which was not designed to evaluate stresses). Without proper explanation, the participant believed that everything provided was needed to complete the test. Improving the instructions and test presentation was a primary issue moving forward. We addressed this as part of our design review.

6.1.2 Design Review

After the initial pilot, the readiness-test development team met and conducted a review of the test design and artifacts. Our goal was to evaluate areas where the instructions, presentation, and design of the test could be made more effective. During this review, we reached the following conclusions:

- We need to provide the participant with written instructions describing the scenario being tested as well as the participant's role in that scenario. Oral instructions from the test administrator are not sufficient. Providing written instructions to participants helps to ensure that the test is explained in a clear and consistent manner to all participants.

[17] Our target audience members are newly graduated security analysts who have acquired some degree of real-world experience by participating in a fellowship program. During the fellowship program, participants spend time working with a team of forensic analysts to gain some real-world forensic experience.

- We need to conduct a detailed walk-through of the equipment and reference materials with the participant before beginning the test. The test administrator needs to point out that the participant will not need to use all of the equipment and artifacts in the testing environment. The test administrator also needs to emphasize the unstructured nature of the test and encourage the participant to ask questions as needed.

After the design review, we updated the instruction set for the scenario and prepared to conduct the second internal pilot.

6.1.3 Pilot 2: Experienced Analyst

The participant in our second pilot was a computer scientist with considerable theoretical and practical experience in the discipline of information security. This participant was considerably more experienced than someone from our target audience. Here, we wanted to gauge how an experienced participant might react to the readiness test. While the readiness test is designed for a forensic analyst with limited field experience, we cannot rule out the possibility that experienced, highly capable individuals might be asked to take the test. For example, an organization might require all new employees (regardless of their experience level) to pass a series of readiness tests before being deployed to the field.

For the second pilot, we administered the same readiness test that we used in the first pilot. During the test, the participant asked several probing questions that required extensive knowledge of how to conduct digital investigations and how to use forensic tools. This issue highlights the experience level of the test administrator. Inexperienced test administrators might be unable to adequately answer advanced questions from experienced participants.

In particular, the test administrator needs to be intimately familiar with all tools that are provided to the participant. The administrator needs to understand the nature of all inputs required by the tools as well as all types of outputs produced by the tools. While the readiness test used in our internal pilots is relatively simple, it does require participants to use tools that are capable of performing advanced cyber-forensics functions. An experienced participant could use tool functions with which the test administrator is unfamiliar. This situation can affect the test administrator’s ability to confidently grade the test.

During the pilot, we also noted the potential for experienced participants to be distracted from the task at hand. During the second pilot, the participant began exploring advanced tool functions to see what they would do. In general, experienced participants might experiment with a tool during the test to learn more about the tool’s functions. This can consume valuable test time (if that is a consideration) and distract the participant from the task at hand. It is important to provide clear and concise instructions to advanced participants about how the test will be conducted and, perhaps more importantly, how it will be graded.

6.2 External Pilot

For our external pilot, we conducted two readiness tests with six people who were participating in a government cybersecurity fellowship program. The first was a basic readiness test for forensics data collection; the second was a stress version of the data collection readiness test. The people from the fellowship program are members of our target audience for readiness testing. For this pilot activity, the readiness-test participants (i.e., the six fellows) were provided a variety of forensic tools for their use during the test. However, we did not restrict them to the tool suite that we provided; they were allowed to bring their own tools and reference materials to the test. (In the field, forensic analysts have the ability to select the tools and equipment they intend to use onsite.) The remainder of this subsection describes the results of each readiness test and the lessons we learned from administering the tests.

6.2.1 Basic Readiness Test for Forensic Data Collection

First, we administered the basic readiness test for forensic data collection to each participant. The basic readiness test is designed to evaluate a participant's ability to complete a job task in the absence of any technical or environmental stressors. The goal of the basic test is to determine if a participant can complete a job task under ideal conditions. This test is fundamentally the same one that we used for our internal piloting activities.[18] (For more information on the readiness test administered in this pilot, refer to Appendix A for the readiness scenario and Appendix C for the test design.)

We administered the test to each participant individually. At the beginning of the test, each participant had time to become familiar with the tools that we provided. We also presented the following success criteria to each participant:

- The participant must successfully retrieve an image of volatile memory from the target machine.
- The participant must successfully image the hard drive located in the target machine.

The target machine in this scenario was a Dell desktop computer with a fairly standard enterprise configuration: one hard drive, 4 gigabytes (GB) of random access memory (RAM), and no external data connectors (except for 6 USB ports). The machine was turned on and logged in when presented to each participant at the beginning of the test.

All six participants passed the basic readiness test with little difficulty. In general, participants started the test by examining the tool suite that we provided to them. After participants had become familiar with the available tools, they started to collect data. All participants understood the steps they needed to take to retrieve the volatile memory and image the hard drive. Four out of the six participants took at least 20 minutes to familiarize themselves with the equipment before beginning to capture volatile memory. Two participants elected to not use the tools provided and downloaded tools with which they were more familiar.

6.2.2 Stress Readiness Test for Forensic Data Collection

Unlike the internal pilots, we also conducted a stress readiness test as part of the external pilots. The stress readiness test is a role-playing exercise based on the forensic data-collection scenario. However, in the stress test, the scenario features a barrier (i.e., a stress) that the participant has to overcome.

In the stress scenario for forensic data collection, a forensic team from a government unit is conducting an investigation into malicious cyber activity originating within a large government civil-

[18] The tests used in the internal and external pilots were identical to each other from a technical perspective. However, we provided more detailed verbal and written instructions for the external pilot participants. These were improvements that we identified during our internal pilots.

ian agency. The readiness-test participant plays the role of a team member who travels to the government agency's site to collect data from an affected computer. The participant is instructed to collect data from hardware that test administrators have set up in a conference room.

For this test, we included the following stress: RAID (redundant array of independent disks) is implemented in the target machine. (For more information on the readiness test administered in this pilot, refer to Appendix B for the readiness scenario and Appendix D for the corresponding test design.)

We administered the stress readiness test to each participant individually. At the beginning of the test, each participant had time to become familiar with the tools that we provided. The success criteria for this scenario are

- The participant must successfully retrieve an image of volatile memory from the target machine.
- The participant must capture a logical image of the hard drive.

For the stress test, participants were instructed to collect the data from an enterprise Dell workstation. This target machine was presented to the students turned on and logged in. However, the workstation operated on a RAID-0 configuration. Instead of having one physical drive, the workstation has two hard-drives each storing half the data.[19] If a participant decides to image each drive by itself, he or she would not collect meaningful data.[20] It is generally considered best practice to conduct what is called a "live-image," where a disk is imaged while the computer is turned on and operating. When captured this way, a logical copy of the drive is retrieved.

Five of the six participants passed the stress readiness test. However, of the five participants that passed the test, four came very close to failing. Those four participants did not immediately realize how the RAID array would affect their data collection procedures. In fact, three did not recognize that they would need to perform a live image after they had already begun collecting volatile memory. The student who failed the exercise understood the concept of a RAID array but forgot how to properly image the drive.

6.3 Lessons Learned from the External Pilot

After conducting the external pilot of the data-collection readiness tests, we held a postmortem to identify the key lessons that we learned from the pilot. In the end, we focused on the following three lessons:

Lesson 1: Add failure criteria to grading.

Lesson 2: Evaluate core competencies in readiness tests.

Lesson 3: Tailor readiness tests to counteract unintended stresses.

In the remainder of this section, we provide a brief summary of each lesson, beginning with the importance of defining failure criteria.

[19] The purpose behind a RAID-0 setup is to offer increased hard drive performance. Because mechanical drive speed is often the limiting factor in hard drive performance, a RAID-0 setup allows two disks to perform the data reading mechanics at the same time.

[20] To remedy this situation, the RAID array would have to be reconstructed in a lab using the proper RAID controller. While reconstructing a RAID array is possible (and can be easy to do); it can also be quite difficult to accomplish because RAID arrays can be very large in size and can have unusual configurations.

6.3.1 Lesson 1: Add Failure Criteria to Grading

To capture volatile memory in a forensically sound manner, an analyst must collect it while minimizing his or her interactions with the target machine. Each interaction with a computer leaves a trace in memory, which could overwrite memory that contains actions taken by an attacker. As a result, an attacker's actions would be lost forever. As a rule of thumb, if volatile memory is to be collected, the forensic analyst should always be sure to collect it first.

In our external pilot, one participant did not know this rule of thumb and began imaging the hard drive before collecting volatile memory from the machine during the basic readiness test. In an investigative setting, this action would have compromised the .mem file from the machine's RAM. However, we did not account for this situation in our grading criteria.

For the external pilot, we graded each readiness test using the prescribed success criteria for that test. (See Sections 6.2.1 and 6.2.2 for each test's success criteria.) We believed that these would be sufficient to use to determine a participant's grade (i.e., pass or fail). However, as described above, one participant imaged the hard drive before retrieving the volatile memory. At the conclusion of the test, that participant had imaged the hard drive and collected the volatile memory (thus meeting the success criteria).

By performing these actions in the wrong order, the participant compromised data stored in the computer's RAM. This mistake could be costly in the field and might be grounds for failing the participant taking the test. However, our grading criteria were not sufficiently nuanced to consider the impact of this mistake.

Our lesson is to augment the success criteria used to grade the test with failure criteria. The following is a prototype list of possible failure criteria for the two readiness tests:

- The participant turns off the machine before collecting volatile memory.
- The participant attempts to image the hard drive before collecting volatile memory.[21]
- The participant installs any program to the local drive of the target machine.
- The participant fails to document his or her interactions with the target computer.
- The participant causes catastrophic damage to the target machine, including but not limited to
  - getting the target machine wet
  - causing electrical damage to the target machine
  - physically harming a hard drive or any of its constituent connectors to the point it is no longer usable
  - physically harming the RAM to the point it is no longer usable

For the stress readiness test, we identified one additional candidate failure criterion: The participant turns off the machine before collecting a logical image of the hard drive. A participant would thus fail a readiness test whenever he or she (1) fails to meet any of the specified success criteria or (2) meets any of the specified failure criteria.

[21] In some instances, an analyst might need to image the hard drive before collecting volatile memory. For example, when dealing with hard disk encryption, an analyst might decide to capture the hard disk information first if he or she is concerned about the system crashing. A crash while capturing volatile memory would result in the encrypted hard disk becoming inaccessible without proper credentials.

6.3.2 Lesson 2: Evaluate Core Competencies in Readiness Tests

We identified communication as a core company for the forensic data-collection scenarios upon which the readiness tests are based. More specifically, a key behavioral indicator for these scenarios is documenting information and keeping good records. Taking effective notes is an important aspect of forensic data collection. As used in this context, the “notes” include both written records of actions taken during data collection as well as visual documentation (i.e., photographs) of the computer and its surroundings.

Our lesson is to make documentation of the data collection activity (both notes and pictures) an integral part of the two readiness tests. To enable note taking, we intend to (1) provide materials to record actions taken during each test, (2) provide cameras for visually documenting the computer and its surroundings, and (3) define appropriate success and failure criteria for note taking and record keeping.

6.3.3 Lesson 3: Tailor Readiness Tests to Counteract Unintended Stresses

The basic and stress readiness tests administered during the external pilot did not include time limits as a stress. Each test was designed to enable the participant to complete it at his or her desired pace. However, logistical issues for the external pilot limited testing time to a total of four hours for each participant to complete both tests. While this might seem like a generous amount of time for two relatively simple forensic tasks, forensic tools can take considerable time to image a hard drive. In addition, the older hardware we provided for the tests increased the amount of time needed to image a hard drive.

To mitigate the effect of the time constraint, we tailored the tests to ensure that the time limits would not affect the results. We decided to omit certain activities in the test and substitute short quizzes for those activities. For example, after a participant had set up and started the imaging process, we quizzed him or her about the subsequent steps that they would take after the imaging was complete.

The key lesson is to be aware of the effect the testing environment might have on the results of the readiness tests. It is important to be flexible and find ways to tailor the testing process to reduce or eliminate the effects of unintended stresses.

7 Summary and Next Steps

Throughout this report, we have emphasized two concepts that are integral to workforce effectiveness: competence and readiness. *Competence* is the sufficient mastery of the knowledge, skills, and abilities needed to perform a given task. It reflects how well an individual understands subject matter or is able to apply a given skill. *Readiness* is the ability to apply the total set of competencies (technical and core) required to perform a job task in a real-world environment with acceptable proficiency. Most job tasks require an individual to synthesize information about multiple subjects and apply multiple skills simultaneously. Readiness is focused on the ability to apply a set of technical and core competencies to complete a job task. Our conceptual foundation for workforce readiness is the CLR.

The CLR provides an agile, practical approach to developing and managing a competency-based staff-readiness program. It comprises five core activities—assess, plan, acquire, validate, and test readiness—and two foundational elements that support the activities—criteria and environment. We designed the CLR around the idea that staff members at all levels of expertise require periodic readiness assessments for both existing and anticipated work requirements. The CLR provides a strategy for maintaining and enhancing workforce readiness over time. Central to that strategy is the concept of readiness testing.

A readiness test is a real-world evaluation of whether a person can perform a specific job task as required. Rather than evaluating individual competencies in isolation, a readiness test assesses an individual's ability to apply a group of technical and core competencies needed to perform and excel at a job task. These tests are derived from scenarios that describe how to complete a given job task in its real-world context.

The readiness test development method provides a structured, systematic approach for constructing and piloting readiness tests. As illustrated in Table 10, the method is divided into two parts and ten steps. Part 1 of the method focuses on data collection, where the goal is to collect data from SMEs about what constitutes readiness for specific job tasks. These data provide the basis for test development, which is the goal of Part 2.

Table 10: Summary of the Readiness Test Development Method: Parts and Steps

Part	Step
Part 1: Collect Readiness Data	1.1 Characterize the Role Being Analyzed
	1.2 Identify Important Job Tasks
	1.3 Select a Job Task to Analyze in Detail
	1.4 Analyze the Selected Job Task
	1.5 Identify Barriers for the Selected Job Task
	1.6 Identify KSAs for the Selected Job Task
Part 2: Develop Readiness Scenarios and Tests	2.1 Develop Readiness Scenarios
	2.2 Validate Readiness Scenarios
	2.3 Design and Develop Readiness Tests
	2.4 Evaluate Readiness Tests

We selected the role of forensic analyst (also called digital media analyst) for our initial application of the readiness test development method. We decided during Part 1 of the method to develop readiness tests for forensic data collection, a high-priority job task performed by forensic analysts.

We developed two readiness tests for forensic data collection: a basic test and a stress test. The basic readiness test is a role-playing exercise based on a forensic data-collection scenario. In that scenario, a forensic team from a government unit is conducting an investigation into malicious cyber activity originating within a large government civilian agency. The readiness-test participant plays the role of a team member who travels to the government agency's site to collect data from an affected computer. The participant is instructed to collect data from hardware that test administrators have set up in a conference room. For the stress readiness test, we included the following stress: RAID (redundant array of independent disks) is implemented in the target machine.

We conducted internal and external pilots of the readiness tests. For the internal pilot, we recruited two technical staff members from our organization: one novice security analyst and one highly experienced security analyst. For the external pilot, we conducted the basic and stress readiness tests with six people who were participating in a government cybersecurity fellowship program. The people from the fellowship program are members of our target audience for readiness testing.

After completing the external pilot, we held a postmortem to identify the key lessons that we learned from all of our piloting and review activities. In the end, we focused on the following three lessons:

Lesson 1: Add failure criteria to grading.

Lesson 2: Evaluate core competencies in readiness tests.

Lesson 3: Tailor readiness tests to counteract unintended stresses.

We plan to incorporate the three lessons into future pilots of the readiness test for forensic data collection. In addition, we have started to apply the readiness test development method to a second role—malware analyst. As we were writing this report, we began the process of collecting data from malware analysts about the tasks that they perform on a daily basis. We then developed a readiness scenario focused on one task in particular—reverse engineering a piece of malware. In the future, we would like to develop a readiness test for reverse engineering and pilot it with our target audience.

The CLR and the readiness test development method are early in their development. Our next step for the CLR includes exploring how to describe each activity and foundational element of the roadmap in more detail. For our readiness testing work, we would like to refine and complete our work on the forensic and malware tests. Beyond that, we would like to expand our readiness testing research and development activities to other cybersecurity roles.

From a broader perspective, additional next steps might include

- expanding readiness testing to evaluated additional cybersecurity technical and leadership roles
- codifying the readiness test development method and transitioning it to the training and development community
- piloting applications of the CLR in smaller settings with individual teams or work groups

- using the CLR in a variety of benchmarking situations that might include training and curriculum design as well as mentoring and supervisory programs
- developing an assessment instrument to allow organizations to benchmark their training and development programs against the CLR so they can identify areas for improvement
- exploring, in conjunction with other groups in the CERT Division, how this readiness approach can be applied to a team rather than to an individual as described in this technical note
- exploring how the CLR can be applied to cybersecurity training and development

This report concludes our initial phase of research and development related to the CLR and readiness testing. The readiness tests that we developed were designed to evaluate an individual's ability to apply the competencies required to perform a job task in a real-world environment with acceptable proficiency. However, more development and piloting is needed to validate the approach. Overall, we believe that this work holds considerable promise for the future. In the years to come, we hope to build on the foundational work described in this report.

Appendix A Example Readiness Scenario for Forensic Data Collection (Basic Version)

Scenario

An investigation has identified malicious cyber activity originating within the ABC Branch of a large government civilian agency. A team from a government unit has been assigned to investigate the malicious activity. The lead investigator has already met with management from both the agency and the branch, and has received written consent to collect data from the agency's computers and networks to support the investigation. J. Smith is one of the investigators on the team.

The lead investigator has asked Smith to visit the ABC Branch's facility and image a computer's hard drive located at the site. Smith has completed background research on the ABC Branch to better understand its mission and how it is organized. In addition, Smith has read the consent document and met with the lead investigator to better understand the assignment. Smith has the written consent in hand and has arranged to meet a member of the ABC Branch's IT staff onsite.

When Smith arrives at the site, an IT staff member is waiting and escorts Smith to a conference room. A manager familiar with the branch's business operations is waiting for Smith in the room. Smith presents the written consent to the group of people assembled in the conference room. Smith and the site personnel then proceed to discuss which data will be collected and the devices to which Smith will need access. During the discussion, Smith asks the following types of questions to gather additional information:

- How is the computer configured (hardware and software)?
- Where are the files of interest (both business and IT files) located on the hard drive?
- What types of applications are running on the hard drive?
- What other data might be of interest to the investigation (e.g., log files)?
- Is any encryption being used?
- Which network(s) is the computer plugged into?

After the meeting ends, the IT staff member escorts Smith to the requested computer. This particular computer was used by the malicious actor to commit the act that is being investigated. The malicious actor is not in the vicinity but is currently logged in and the computer is unlocked. At this point, Smith is ready to begin the process of imaging the hard drive. First, Smith focuses on the computer's volatile memory. Smith attaches a collection device to the malicious actor's computer via the USB port and, using a physically connected collection tool, begins copying volatile memory from the computer's RAM.

Next, Smith shuts down the computer and removes its hard drive. (Smith can image the computer when it is powered down because data on the hard drive are not encrypted and RAID is not implemented.) Smith puts the hard drive into a write block and then images the drive. The forensic tool that Smith uses automatically hashes the image. Smith verifies that the hash value for the copy matches that of the hard drive. Smith then creates a backup of the forensic image by copying the image to another hard drive.

Smith also takes these careful notes during the session:

- the make, model, serial number, and MAC address of the computer
- what is connected to the computer (e.g., power, keyboard)
- what actions were taken and when
- the initial condition of the computer (e.g., unlocked, unencrypted)
- what screens are open on the computer
- screen captures of running processes
- the time and date that volatile memory was collected

Smith also makes sure to take photographs to visually document the initial state of the actor’s computer (including photos of any peripherals connected to the computer). Finally, Smith puts both drives (i.e., the drive with the forensic image and the drive with the copy of the forensic image) into static bags for transport. At this point, Smith has completed data collection for this investigation and is ready to take the evidence back to the lab for analysis. The IT manager signs a document that describes the data collected by Smith. When transporting the evidence, Smith preserves the chain of custody along the way.

Technical Competencies

Competency	Behavioral Indicator
Investigation	Apply knowledge of chain-of-custody practices (e.g., knowing the sign-off procedures for data)
	Apply knowledge of evidential procedures (e.g., do not boot the hard drive if you don’t have to)
Digital Forensics	Apply knowledge of system administration concepts
	Apply knowledge of hard drives and file systems (e.g., how data are written to drives)
	Apply knowledge of data-collection practices for digital investigations
	Image a hard drive
	Collect volatile data (e.g., data in system registers, cache, RAM)
	Use imaging tools (e.g., dd, dc3dd, FTK imager, EnCase acquisition)
	Use hash values (e.g., MD5)

Core Competencies

Competency	Behavioral Indicator
Communication	Document information and keep good records
	Communicate with team members (including the team leader)
	Communicate with onsite stakeholders (e.g., IT staff, management)
	Gather information about a situation by asking effective questions
Technical Proficiency	Apply knowledge of the business and mission of the organization being investigated (e.g., organizational structure, knowing who is responsible for what)
	Solve problems
	Use support tools (e.g., Word, Excel) when documenting information
	Attend to detail when performing work tasks

Appendix B Example Readiness Scenario for Forensic Data Collection (Stress Version)

Scenario

An investigation has identified malicious cyber activity originating within the ABC Branch of a large government civilian agency. A team from a government unit has been assigned to investigate the malicious activity. The lead investigator has already met with management from both the agency and the branch, and has received written consent to collect data from the agency's computers and networks to support the investigation. J. Smith is one of the investigators on the team.

The lead investigator has asked Smith to visit the ABC Branch's facility and image a computer's hard drive located at the site. Smith has completed background research on the ABC Branch to better understand its mission and how it is organized. In addition, Smith has read the consent document and met with the lead investigator to better understand the assignment. Smith has the written consent in hand and has arranged to meet a member of the ABC Branch's IT staff onsite.

When Smith arrives at the site, an IT staff member is waiting and escorts Smith to a conference room. A manager familiar with the branch's business operations is waiting for Smith in the room. Smith presents the written consent to the group of people assembled in the conference room. Smith and the site personnel then proceed to discuss which data will be collected and the devices to which Smith will need access. During the discussion, Smith asks these questions to gather additional information:

- How is the computer configured (hardware and software)?
- Where are the files of interest (both business and IT files) located on the hard drive?
- What types of applications are running on the hard drive?
- What other data might be of interest to the investigation (e.g., log files)?
- Is any encryption being used?
- Which network(s) is the computer plugged into?

After the meeting ends, the IT staff member escorts Smith to the requested computer. This particular computer was used by the malicious actor to commit the act that is being investigated. The malicious actor is not in the vicinity but is currently logged in and the computer is unlocked. At this point, Smith is ready to begin the process of imaging the volatile memory hard drive. First, Smith focuses on the computer's volatile memory. Smith attaches a collection device to the malicious actor's computer via the USB port and, using a physically connected collection tool, begins copying volatile memory from the computer's RAM.

During the discussion in the conference room, the IT staff member indicated that the target machine's operating system is installed on a RAID-0 array comprising two physical hard drives. The IT staff member also tells Smith that no other operating systems are running on the logical drive and that the RAID controller used to construct the RAID array is not available.

Because RAID is implemented and RAID controller information is not immediately available, Smith conducts a live image of the hard drive. The forensic tool that Smith uses automatically hashes the image. Smith verifies that the hash value for the logical copy matches that of the two physical hard drives. Smith then creates a backup of the forensic image by copying the image to another hard drive.

Smith also takes these careful notes during the session:

- the make, model, serial number, and MAC address of the computer
- what is connected to the computer (e.g., power cables, keyboard)
- what actions were taken and when
- the initial condition of the computer (e.g., unlocked, unencrypted)
- what screens are open on the computer
- screen captures of running processes
- the time and date that volatile memory was collected

Smith also makes sure to take photographs to visually document the initial state of the actor's computer (including photos of any peripherals connected to the computer). Finally, Smith puts both drives (i.e., the drive with the forensic image and the drive with the copy of the forensic image) into static bags for transport. At this point, Smith has completed data collection for this investigation and is ready to take the evidence back to the lab for analysis. The IT manager signs a document that describes the data collected by Smith. When transporting the evidence, Smith preserves the chain of custody along the way.

Technical Competencies

Competency	Behavioral Indicator
Investigation	Apply knowledge of chain-of-custody practices (e.g., knowing the sign-off procedures for data)
	Apply knowledge of evidential procedures (e.g., do not boot the hard drive if you don't have to)
Digital Forensics	Apply knowledge of system administration concepts
	Apply knowledge of hard drives and file systems (e.g., how data are written to drives)
	Apply knowledge of data-collection practices for digital investigations
	Apply knowledge of RAID
	Perform live imaging of hard drive
	Collect volatile data (e.g., data in system registers, cache, RAM)
	Use imaging tools (e.g., dd, dc3dd, FTK imager, EnCase acquisition)
	Use hash values (e.g., MD5)

Core Competencies

Competency	Behavioral Indicator
Communication	Document information and keep good records
	Communicate with team members (including the team leader)
	Communicate with onsite stakeholders (e.g., IT staff, management)
	Gather information about a situation by asking effective questions
Technical Proficiency	Apply knowledge of the business and mission of the organization being investigated (e.g., organizational structure, knowing who is responsible for what)
	Solve complex problems
	Use support tools (e.g., Word, Excel) when documenting information
	Attend to detail when performing work tasks

Scenario Stresses

Stress		Task-Specific Competencies	Enabling Competencies
1	RAID is implemented in the computer of interest.	Knowledge of RAID Ability to live image a hard drive	---

Appendix C Example Readiness Test Design for Forensic Data Collection (Basic Version)

Success Criteria

The following are the success criteria for this readiness test:

- Participants successfully capture an image of the hard drive from the designated computer, and the hash of the image matches the hash of the original hard drive.
- Participants successfully capture RAM from the designated computer.
- Participants document basic notes describing what they did to collect the data and when. At a minimum, the following items must be documented:
  - hash value for the hard drive and the copy of the hard drive
  - times when the imaging occurred and various systems were accessed

Test Format

The test is a role-playing exercise. Participants collect data from hardware that is set up in a room.

The test includes the following roles:

- *data collector*—The data collector is the person performing the data collection.
- *site personnel*—At least two site roles are specified: (1) an IT staff member and (2) a business operations manager.

The participant (i.e., the person taking the test) plays the role of data collector. Multiple participants can work as a team to collect the data, when appropriate. Multiple test administrators can play the role of site personnel. Alternately, a single test administrator can assume all roles.

Equipment

- Desktop with Windows 7 and a forensic "flag" consisting of a file split into five parts with randomly corrupted file headers
  - mouse and keyboard
  - no network access
  - 80 GB Hard disk
  - 4x SATA to SATA connectors
  - DVD disk drive
  - 6x USB connectors
- Drive write blocks for physical imaging of the hard drive
  - Tableau Imaging Bridge
  - Voom Hardcopy III
- 5x250 GB SATA hard disks

- SATA to SATA connectors (x4)
- Raptor Forensics Kit boot-disk
- ADAI Forensics Kit boot-disk

Software

- Operating Systems
  - Windows 7
  - CERT Linux Forensics Appliance
  - Raptor Forensics OS
- Other Software
  - FTK Forensics Tool Kit
  - FTK Forensics Imager Lite
  - Autopsy Forensics Tool Kit
  - VM Player
  - Virtual Box
  - 7-Zip
  - Olly Debugger

Sequence of Events

Event	Description
1. Preparation	This step is conducted before the participant comes to the testing site. Before the test, the lead test administrator sends an email to the participant to let him/her know which forensic tools will be provided for the test. In the email, the lead test administrator also lets the participant know that he/she can bring his/her own forensic toolkit, if desired.
2. Test Start	This step begins with the participant arriving at the testing site. The participant enters the testing room. The lead test administrator describes the test and the role that the participant is playing. The lead test administrator provides the participant with a handout that describes the role of data collector. The lead test administrator describes what is expected of the participant during the data-collection activity. (See role descriptions for details.)
3. Hardware Discussion	The lead test administrator shows the participant the hardware to be used during the data collection activity. The lead test administrator asks the participant if he/she is familiar with the equipment and asks if he/she has any questions about the equipment. The lead test administrator provides the participant a few minutes to become familiar with the equipment.
4. Questioning Site Personnel	The data-collection activity begins as the test administrators assume their roles for the test. (The lead test administrator can assume all roles, if desired.) The participant needs to ask questions of the site personnel (played by the test administrators) to get the information that he/she needs to collect the data (e.g., what data to collect, where the data are located).

Event	Description
5. Data Collection	The participant performs the data collection activity. The participant captures RAM from the designated computer. The participant also captures an image of the hard drive from the designated computer. He/she then makes sure that the hash of the image matches the hash of the original hard drive. As needed, the participant asks site personnel questions relevant to performing the data-collection activity. The participant also documents basic notes describing what he/she did to collect the data and when. Finally, at the conclusion of data collection, the participant packs the drive with the copied image in a static bag for transport.

Time Constraints

No time limits exist for this test.

Materials Required

- Description of the role of data collection
- Description of each site role (IT staff member and business operations manager)
- Notebook and pen (for participants to document notes during test)

Appendix D Example Readiness Test Design for Forensic Data Collection (Stress Version)

Success Criteria

The following are the success criteria for this readiness test:

- Participants successfully capture an logical (single drive) image of the RAID-0 array from the designated computer
- Participants successfully capture RAM from the designated computer
- Participants document basic notes describing what they did to collect the data and when. At a minimum, the following items must be documented:
  - hash value for the hard drive and the copy of the hard drive
  - times when the imaging occurred and various systems were accessed

Test Format

The test is a role-playing exercise. Participants collect data from hardware that is set up in a room.

The test includes the following roles:

- *data collector*—The data collector is the person performing the data collection.
- *site personnel*—At least two site roles are specified: (1) an IT staff member and (2) a business operations manager.

The participant (i.e., the person taking the test) plays the role of data collector. Multiple participants can work as a team to collect the data, when appropriate. Multiple test administrators can play the role of site personnel. Alternately, a single test administrator can assume all roles.

Equipment

- Desktop with Windows 7 and a forensic "flag" consisting of a file split into five parts with randomly corrupted file headers
  - mouse and keyboard
  - no network access
  - 2x80 GB Hard disks
  - 4x SATA to SATA connectors
  - DVD disk drive
  - 6x USB connectors
- Drive write blocks for physical imaging of the hard drive
  - Tableau Imaging Bridge
  - Voom Hardcopy III
- 5x250 GB SATA hard disks

- SATA to SATA connectors (x4)
- Raptor Forensics Kit boot-disk
- ADAI Forensics Kit boot-disk
- Ubuntu Boot Disk

Software

- Operating Systems
  - Windows 7
  - CERT Linux Forensics Appliance
- Other Software
  - FTK Forensics Tool Kit
  - FTK Forensics Imager Lite
  - Autopsy Forensics Tool Kit
  - VM Player
  - Virtual Box
  - 7-Zip
  - Olly Debugger

Sequence of Events

Event	Description
1. Preparation	This step is conducted before the participant comes to the testing site. Before the test, the lead test administrator sends an email to the participant to let him/her know which forensic tools will be provided for the test. In the email, the lead test administrator also lets the participant know that he/she can bring his/her own forensic toolkit, if desired.
2. Test Start	This step begins with the participant arriving at the testing site. The participant enters the testing room. The lead test administrator describes the test and the role that the participant is playing. The lead test administrator provides the participant with a handout that describes the role of data collector. The lead test administrator describes what is expected of the participant during the data-collection activity. (See role descriptions for details.)
3. Hardware Discussion	The lead test administrator shows the participant the hardware to be used during the data collection activity. The lead test administrator asks the participant if he/she is familiar with the equipment and asks if he/she has any questions about the equipment. The lead test administrator provides the participant a few minutes to become familiar with the equipment.

Event	Description
4. Questioning Site Personnel	The data-collection activity begins as the test administrators assume their roles for the test. (The lead test administrator can assume all roles, if desired.) The test administrator playing the role of information technology (IT) staff member should inform the participant of the following pieces of information: ▪ The target machine’s operating system is installed on a RAID-0 array comprising two physical hard drives. ▪ No other operating systems are running on the logical drive. ▪ The RAID controller used to construct the RAID array is not available. The participant should ask questions of the site personnel (played by the test administrators) to get additional information that he/she needs to collect the data (e.g., what data to collect, where the data are located).
5. Data Collection	The participant performs the data collection activity. The participant captures RAM from the designated computer. Because RAID is implemented and RAID controller information is not immediately available, the participant must conduct a live image of the hard drive. He/she then makes sure that the hash of the image matches the hash of the two original hard drives. As needed, the participant asks site personnel questions relevant to performing the data-collection activity. The participant also documents basic notes describing what he/she did to collect the data and when. Finally, at the conclusion of data collection, the participant packs the drive with the copied image in a static bag for transport.

Time Constraints

No time limits exist for this test.

Materials Required

- Description of the role of data collection
- Description of each site role (IT staff member, business operations manager, data collector)
- Notebook and pen (for participants to document notes during test)

Bibliography

URLs are valid as of the publication date of this document.

[Behrens 1992]
Behrens, S. & Crossman, D. "Affective Strategies for Effective Learning," *Proceedings of the Annual Conference of the Association for Educational Communications and Technology*, Washington, DC, February 12, 1992.

[Behrens 2004]
Behrens, Sandra; Mogilensky, Judah; & Masters, Steve. *CMMI-Based Professional Certifications: The Competency Lifecycle Framework* (CMU/SEI-2004-SR-013). Software Engineering Institute, Carnegie Mellon University, 2004.
http://www.sei.cmu.edu/library/abstracts/reports/04sr013.cfm

[Behrens 2012]
Behrens, Sandra; Alberts, Christopher; & Ruefle, Robin. *Competency Lifecycle Roadmap: Toward Performance Readiness* (CMU/SEI-2012-TN-020). Software Engineering Institute, Carnegie Mellon University, 2012.
http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=28053

[Blank 1982]
Blank, William E. *Handbook for Developing Competency-Based Training Programs*. Prentice Hall, 1982.
http://books.google.com/books/about/Handbook_for_Developing_Competency_Based.html?id=kgmfAAAAMAAJ

[Curtis 2002]
Curtis, B.; Hefley, W.; & Miller, S. *The People Capability Maturity Model - Guidelines for Improving the Workforce*. Addison-Wesley, 2002.
http://www.informit.com/articles/article.aspx?p=25349

[Dijkstra 1989]
Dijkstra, S.; Van Hout-Wolters, W.; & Van Der Sijde, P. *Research on Instruction: Design and Effects.* Educational Technology Publications, 1989.
http://books.google.com/books?hl=en&lr=&id=AjuqO8S5drYC&oi=fnd&pg=PR5&dq=Research+on+Instruction:+Design+and+Effects&ots=BdxZVGKfxV&sig=llwogkm11PigUQoPfWgXevgHruQ

[Gott 2000]
Gott, S.P. & Lesgold, A.M. "Competence in the Workplace: How Cognitive Performance Models and Situated Instruction Can Accelerate Skill Acquisition," Ch. 5, 239-329. *Advances in Instructional Psychology – Vol. 5: Educational Design and Cognitive Science*, Lawrence Erlbaum Associates, 2000.
http://psycnet.apa.org/psycinfo/2000-05265-005

[Hammerstein 2010]

Hammerstein, Josh & May, Christopher. *The CERT Approach to Cybersecurity Workforce Development* (CMU/SEI-2010-TR-045). Software Engineering Institute, Carnegie Mellon University, 2010.
http://www.sei.cmu.edu/library/abstracts/reports/10tr045.cfm

[Islam 2006]

Islam, K. *Developing and Measuring Training the Six Sigma Way: A Business Approach to Training and Development.* Pfeiffer, 2006.
http://books.google.com/books?hl=en&lr=&id=aeNGg7V82SwC&oi=fnd&pg=PR7&dq=Developing+and+Measuring+Training+the+Six+Sigma+Way:+A+Business+Approach+to+Training+and+Development&ots=z2NZVu7L_1&sig=cilcujkUNXK1Zkb5CJlhMXqDFZQ

[Lajoie 2008]

Lajoie, S. "Metacognition, Self Regulation, and Self-Regulated Learning: A Rose by Any Other Name?" *Educational Psychology Review 20*, 4 (December 2008): 469-475.
http://link.springer.com/article/10.1007/s10648-008-9088-1

[Lesgold 1997]

Lesgold, A.M. *Transitions in Work and Learning: Implications for Assessment.* National Academy Press, 1997.
http://books.google.com/books?hl=en&lr=&id=AUMrAAAAYAAJ&oi=fnd&pg=PR5&dq=Transitions+in+Work+and+Learning:+Implications+for+Assessment&ots=H85KYCo7fS&sig=-h4PSibTcIQpX1knDp81NLl9CPU

[Masters 2007]

Masters, S.; Behrens, S.; Mogilensky, J.; & Ryan, C. *SCAMPI Lead Appraiser Body of Knowledge (SLA BOK)* (CMU/SEI-2007-TR-019). Software Engineering Institute, Carnegie Mellon University, 2007.
http://www.sei.cmu.edu/library/abstracts/reports/07tr019.cfm

[NICE 2011]

National Initiative for Cybersecurity Education (NICE). *Cybersecurity Workforce Framework.* NICE, 2011.
http://csrc.nist.gov/nice/framework/documents/national_cybersecurity_workforce_framework_printable.pdf

[OERI 1994]

Office of Educational Research and Improvement. *The National Assessment of College Student Learning: Identification of the Skills to Be Taught, Learned and Assessed* (NCES 94-286). U.S. Department of Education, 1994.
http://files.eric.ed.gov/fulltext/ED383255.pdf

[OPM 2006]

Office of Personnel Management (OPM). *Leadership Competency Framework.* OPM, 2006.
http://www.ocio.usda.gov/directives/doc/DR4040-412-001.htm

[OPM 2011]
Office of Personnel Management (OPM). *Competency Model for Cybersecurity*. OPM, 2011. http://www.chcoc.gov/transmittals/TransmittalDetails.aspx?TransmittalID=3436

[Patton 1987]
Patton, M. *How to Use Qualitative Methods in Evaluations.* Sage, 1987. http://books.google.com/books?hl=en&lr=&id=shxPj6FxQSoC&oi=fnd&pg=PA5&dq=How+to+Use+Qualitative+Methods+in+Evaluations&ots=gRtQg_Jv6T&sig=XQ_lgrTjYQFCXbnXyrUCSYkgxm0

[PMI 2002]
Project Management Institute. *Project Manager Competency Development Framework*. Project Management Institute, 2002. http://books.google.com/books?id=7MgCAAAACAAJ&dq=Project+Manager+Competency+Development+Framework&hl=en&sa=X&ei=qRBVU5-yJ4GMygGE_YHwDg&ved=0CEIQ6AEwAQ

[Rossett 1998]
Rossett, A. *First Things Fast: A Handbook for Performance Analysis.* Jossey-Bass, 1998.

[SCAMPI 2011]
SCAMPI Upgrade Team. *Standard CMMI Appraisal Method for Process Improvement (SCAMPI) A, Version 1.3: Method Definition Document* (CMU/SEI-2011-HB-001). Software Engineering Institute, Carnegie Mellon University, 2011. http://www.sei.cmu.edu/library/abstracts/reports/11hb001.cfm

[Simon 1996]
Simon, H.A. *The Sciences of the Artificial*, 3rd ed. The MIT Press, 1996.

[Wiggins 2006]
Wiggins, G. & McTighe, J. *Understanding by Design*, expanded 2nd ed. Prentice Hall, 2006.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY
(Leave Blank)

2. REPORT DATE
August 2014

3. REPORT TYPE AND DATES COVERED
Final

4. TITLE AND SUBTITLE
A Systematic Approach for Assessing Workforce Readiness

5. FUNDING NUMBERS
FA8721-05-C-0003

6. AUTHOR(S)
Christopher Alberts and David McIntire

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

8. PERFORMING ORGANIZATION REPORT NUMBER
CMU/SEI-2014-TR-009

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
AFLCMC/PZE/Hanscom
Enterprise Acquisition Division
20 Schilling Circle
Building 1305
Hanscom AFB, MA 01731-2116

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12A DISTRIBUTION/AVAILABILITY STATEMENT
Unclassified/Unlimited, DTIC, NTIS

12B DISTRIBUTION CODE

13. ABSTRACT (MAXIMUM 200 WORDS)

Workforce effectiveness relies on two critical characteristics: competence and readiness. *Competence* is the sufficient mastery of the knowledge, skills, and abilities needed to perform a given task. It reflects how well an individual understands subject matter or is able to apply a given skill. *Readiness* is the ability to apply the total set of competencies required to perform a job task in a real-world environment with acceptable proficiency. A readiness test assesses an individual's ability to apply a group of technical and core competencies needed to perform and excel at a job task. This report describes research into workforce readiness conducted by the Computer Security Incident Response Team (CSIRT) Development and Training team in the CERT® Division of Carnegie Mellon® University's Software Engineering Institute (SEI). This report presents the Competency Lifecycle Roadmap (CLR), a conceptual framework for establishing and maintaining workforce readiness within an organization. It also describes the readiness test development method, which defines a structured, systematic approach for constructing and piloting readiness tests. Finally, the report illustrates the initial application of the readiness test development method to the role of forensic analyst.

14. SUBJECT TERMS
workforce readiness, workforce competence

15. NUMBER OF PAGES
63

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT
Unclassified

18. SECURITY CLASSIFICATION OF THIS PAGE
Unclassified

19. SECURITY CLASSIFICATION OF ABSTRACT
Unclassified

20. LIMITATION OF ABSTRACT
UL