# Workforce Skills Credentialing

## Security Framework Report

## BOOK 2

Association of Test Publishers


# ATP Workforce Skills Credentialing Division

# Credentialing Security Framework

## The Association of Test Publishers

Established in 1992, the Association of Test Publishers ("ATP") is an international non-profit organization representing providers of tests and assessment tools and/or assessment-related services used in clinical, employment, certification, licensure, credentialing, and educational settings.

The ATP's membership is comprised of the leading publishers and assessment services providers in today's testing industry. Presently there are four regional organizations, five practice area divisions and two special interest groups ("SIGs") that are active subgroups of the ATP's global membership. Region organizations exist for Asia, Europe, India, and North America. Practice Area Divisions include Clinical, Certification/Licensure, Industrial/Organizational, Education, and Workforce Skills Credentialing. SIGs cover the Health Sector and Public Sector.

The ATP's regions, divisions, and SIGs provide networking opportunities for members and a forum for specialized areas of the assessment industry represented within the ATP.

The ATP's mission is to promote and preserve the general welfare of testing and its value to society, in all its forms and uses; to organize test publishers into a permanent body to foster and maintain collegial relations among themselves and to establish, through the Association, working relationships with other professional and business groups whose interests and activities affect the test publishing community; to encourage a high level of professionalism and business ethics throughout the testing community; to serve as the principal organization that monitors and responds to regulatory and legal rulings as well as legislative, regulatory, and judicial initiatives that pertain to the business of publishing and applying test and assessment instruments; and to increase the strength and cohesiveness of the test publisher community by providing programs of education, training, and exchanges of ideas on operations and industry trends.

Visit the ATP online at www.testpublishers.org.

# Document Structure and Disclaimer

This document provides general information concerning workforce credentials and initiatives underway to identify common competencies. It provides references to bring greater clarity to the workforce credentialing market and discusses how use of the Credentialing Security Framework brings clarity to the use of workforce credentials. It also provides use cases for key stakeholders within the workforce credentialing ecosystem. Finally, it contains the Credentialing Security Framework, which details six areas of test security and authentication, with four levels of capabilities within each area.

This document is intended only to provide general, high-level guidance concerning the use of a framework communicating information on exam security in the workforce skills credentialing space. A user of this document must consider whether any given section or subsection is applicable to its specific program(s), credential(s), or test(s). While the ATP has made every effort to ensure the information contained in this document has been developed from reliable sources, all information is provided "as is" and neither the ATP, nor any participating publishers or service providers, makes any warranty, express or implied, nor do they collectively or separately assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, product, or process described in this document. In no event will the ATP, its agents, or employees be liable to any user of this document for any decision made or action taken in reliance on the information in this document, including but not limited to liability for any consequential, special, or similar damages, even if the ATP has been advised of the possibility of such damages. The information in this report is provided with the understanding that neither the ATP, nor any individuals who participated in the preparation of this document, shall be deemed to be engaged in rendering legal, technical, psychometric, or assessment advice and services. Therefore, this document should not be used as a substitute for consulting with competent legal, technical, psychometric, or assessment advisers.

## Message from William. G. Harris, CEO, ATP

Workforce skills are critical to the financial health of individuals, as well as businesses and our communities. Given the nature of the global economy, a highly-capable workforce serves the best interests of individuals, employers, learning and training institutions, and the assessment industry. Indeed, every country has a need to take steps to reduce or eliminate the existing skills gaps. Developing and demonstrating highly-skilled individuals is attainable, in part, through the use of assessment-based credentials that document useful and needed skills, attitudes, and behaviors -- and that are reliable, valid, securely issued, and capable of being authenticated.

The ATP established the Workforce Skills Division to help provide guidance in the development of trustworthy and reliable assessment-based workforce credentials. The initial work of the Division has been to establish various working committees, including a committee to focus on security and privacy issues within the credentialing space. This Committee conducted a global survey of credential earners, users, issuers, and test publishers to better understand the perspectives of these stakeholders. The survey results underscore the need for a common security language and framework. The Credentialing Security Framework reflects insights from the survey analysis as well as input from industry experts. It is intended to spark dialogue and improve understanding across the industry, all in an effort to improve trust in and use of assessment-based credentials and, in turn, the global workforce.

## Message from Rachel Schoenig, Workforce Skills Credentialing Security & Privacy Committee Chair

In 2014, the ATP established the Workforce Skills Credentialing Division to help inform the reliable, valid, and secure development of assessment-based workforce credentials. The Security and Privacy Committee of ATP's Workforce Skills Credentialing Division strives to develop a test security and privacy ecosystem that furthers the global delivery, use, and understanding of credentials people can trust.

The number of workforce credentials available today has grown significantly over the last three decades, leading to market confusion and an erosion of trust in the value of some credentials. Because credentials play a valuable role in global, regional, and local economies, several entities have undertaken efforts to help reduce confusion. Those efforts, however, focus primarily on the different competencies being measured. Because security and authentication of credentials have a clear impact on the trustworthiness and usefulness of a credential, providing for common understandings of the different security levels available will enable stakeholders to make informed decisions about the use of credentials in their own business or profession. Understanding that exam security is not a "one-size-fits-all" capability, the Committee set out to bring greater clarity to that aspect of credentialing.

The resulting Credentialing Security Framework is the second phase of a project designed to bring greater clarity to the workforce credentialing market. Part one of the project involved a global survey designed to gather data from credential earners, users, issuers, and test publishers regarding exam security concerns in the credentialing market. Those survey results were used to inform the second phase of the project, which involved the development of the Credentialing Security Framework for workforce skills credentials. The Credentialing Security Framework is designed to be used as a stand-alone guide or together with efforts of other organizations (e.g., Connecting Credentials, the European Commission) to provide greater transparency regarding assessment-based workforce skills credentials. The Committee expects that the promotion and use of the Credentialing Security Framework will better enable employers, employees, and others to make informed decisions about the use of a particular credential in their own business or profession.

# Acknowledgments

The Credentialing Security Framework was developed in conjunction with volunteers across ATP, including the following key contributors:

**Committee Chair: Rachel Schoenig**, Cornerstone Strategies, LLC

**Committee Vice-Chair: Jennifer Geraets**, ACT, Inc.

**Patrick Craven,** City & Guilds

**Jarret Dyer,** College of DuPage

**Chuck Friedman**, PSI

**William G. Harris**, CEO, ATP

**John Kessler**, Accenture

**Bob Mahlman,** Center on Education & Training for Employment, The Ohio State University

**Jamie Mulkey**, Caveon

**Robert Pedigo**, Castle Worldwide, Division Chair

**Dan Rinn**, NTT Training, Past Division Chair

**Jim Sharf,** Employment Risk Advisors, Inc., Metrics Reporting, Inc.

**Roy Swift**, WorkCred

**Alan Thiemann**, Law Office of Alan J. Thiemann

**Alex Tong**, ATA

**Linda Waters,** Prometric

**Tim Vansickle**, Advanced Assessment Systems, Division Secretary

# Table of Contents

## General Overview of Workforce Skills Credentials

Workforce credentials often provide meaningful benefits to countries, communities, learning institutions, employers, and individuals. A credentialing ecosystem enables a country to support the development of a skilled workforce, contributing to a robust economy and enhancing economic health. Today, the same ecosystem supports a growing global economy. Assessment-based credentials can facilitate matching employee job skills with employer job needs. At an individual level, credentials can provide job applicants and employees a means of demonstrating and verifying skills and competencies to potential or existing employers or other users of credentialing information. Credentials in turn can aid employers in making hiring, promotion, and retention decisions and other users, such as educational institutions and training programs, in making informed decisions about candidates for admission. Over the past 30 years, however, the number of workforce skills credential offerings have increased dramatically -- by some estimates over 800% since 1960 -- leaving the market in a state of confusion over how to interpret and use credentials and resulting in employers, individuals, and other stakeholders losing trust in credentials.

To deliver on the benefits offered by workforce credentialing, various organizations have called for greater clarity concerning credentials. For example, the recently published "Connecting Credentials: A Beta Connecting Credentials Framework" (Lumina Foundation, 2015), developed by experts from the Corporation for a Skilled Workforce and the Center for Law and Social Policy, provides a common language and competency reference point to enable comparisons across levels of knowledge, skills, and abilities across the full spectrum of credentials. The European Commission has similarly developed eight competences for lifelong learning. These efforts strive to bring some order to the market, offering a common language and framework for stakeholders in the credentialing space. This Credentialing Security Framework provides additional key information to further the goal of clear and transparent credentials. As such, the Credentialing Security Framework can be used by credential earners and users to clarify the meaning of, and enable comparison of, various credentials, or it can be a contributing component to a larger mosaic.

## Why do we need a security framework for credentials?

While the competency frameworks noted above can bring additional clarity to the credentialing space, they do not address the exam security and authentication processes associated with assessment-based credentials. Because security and authentication have a significant impact on the trustworthiness and usefulness of a credential, providing greater transparency concerning the security level of a credential enables stakeholders to make informed decisions about the value of credentials in their own business or profession. Further, just as credentials vary in the range of profiles of competencies tested, the levels of exam security and authentication vary as well. In short, exam security is not a "one-size-fits-all" proposition. Thus, identifying the level of exam security and authentication associated with an assessment-based credential will bring greater clarity to the market. For employers or potential credential earners attempting to choose among the various credential offerings available in the market, knowing the security/authentication associated with a credential enables more effective comparisons and better informed decisions and increases trust in and use of credentials.

The initial phase of this ATP project was a survey of employers, employees, credential issuers, and test publishers -- the key stakeholders involved in the workforce skills credentialing ecosystem. Of the employers who use workforce skills credentials, nearly all respondents indicated it is very important that the credential is authentic (not a forgery) and earned without cheating. Further, the majority indicated it is very important that they have a way to verify the authenticity of a credential and are able to determine if a credential is invalidated or expires. Similarly, nearly all employees indicated it is very important that credentials are earned without cheating and that employers are notified when there are authenticity concerns. Credential issuers and test publishers provide mechanisms for employers or employees to raise authentication and assessment concerns; however, most employers and employees are unaware of those mechanisms. Providing additional information through a security framework will help connect the needs of employers and employees with the practices of credential issuers and test publishers, promote better decision-making and appropriate use of credentials, and increase trust in credentials.

## How was the Credentialing Security Framework developed?

The Workforce Skills Credentialing Division provides expertise and guidance to the expanding credentials market. In furtherance of that mission, the Division's Security and Privacy Committee (the "Committee") sought to enhance credential transparency and quality by creating a set of common exam security/authentication levels that can align the expectations of the various stakeholders involved with workforce credentialing. The Committee approached the project by placing the credential earner and credential user at the center of the process and evaluating their mutual, shared needs for accurate and trustworthy credentials. To better understand the perspectives of the credential earner and credential user, as well as the credential issuer and test publisher, a survey was conducted over a period of four months, from October 2016 to January 2017. The results of the survey informed and shaped the language of the Credentialing Security Framework. The Credentialing Security Framework was developed through multiple reviews and extensive input from stakeholders across the industry. It is intended to work independent of or in conjunction with other frameworks in development, including "Connecting Credentials: A Beta Connecting Credentials Framework."

During development, the Committee recognized the wide variety in assessment security practices currently used across the industry. The Credentialing Security Framework is intended to organize these practices – such as item and exam protection, examinee identification, score validity, administration security, and credential authentication practices, among others – in such a way as to yield greater understanding across all key stakeholders. Each level should be taken as a general body of capabilities that provide a level of assessment security, starting with minimal to no security and advancing to strong security. As such, some of the practices mentioned, while currently used, are not necessarily best practices in the industry. The intent is not to prescribe specific practices or standards, but rather to group what is and can be done for assessment security and allow that information to inform the market. Further, the Committee recognized the speed with which technology changes can date a document such as this. Thus, the Credentialing Security Framework provides examples of current technologies or types of tools in each area, with the understanding these will evolve as technology evolves. While the industry may continue to mature to such a point that standards will develop, this document is a general framework designed to improve communication and drive understanding across the full ecosystem of credentialing. There is no credentialing or certifying body to enforce these security levels; rather, credential issuers and test publishers will be able to self-identify where their credentials fall within the Credentialing Security

Framework.  That information, it is expected, will help enhance the understanding, trustworthiness, and appropriate use of assessment-based credentials within the workforce credentialing market.

# Definitions

Terms are defined as they are used in the Credentialing Security Framework.

- Assessment: A systematic method to obtain information used to draw inferences concerning a credential earner's proficiency in knowledge, skills, abilities, attitude, behavior, or competencies. In this document, assessment is used interchangeably with the terms "test" and "exam."
- Credential Earner: The individual to whom an assessment-based credential is issued. Often, credentials are earned by employees or potential employees, or candidates for specific programs such as educational, professional, or training programs.
- Credential Issuer: The entity that issues a credential that is based in whole or in part on the results of an assessment, such as adult education programs, community colleges, for-profit institutions, and training programs. This term also includes vendors and contractors acting on the credential issuer's behalf, such as delivery vendors and test administrators. The Framework is not necessarily intended to apply to credential issuers who do not use assessments.
- Credential User: Any entity that gives consideration to a workforce skills credential during decision-making. Often, this is an employer, but a credential user may also include government agencies, schools, and others.
- Employee: Includes individuals who are currently gainfully employed, individuals seeking employment or advancement within the job market, and individuals in education and training programs for the purpose of gainful employment upon completion.
- Employer: Includes human resource professionals and other individuals with hiring, promotion, retention, and termination responsibilities.
- Test Publisher: The entity responsible for developing the assessment, the results of which are used by the credential issuer to measure knowledge, skills, abilities, attitude, behavior, or competencies for purposes of issuing a credential.
- Test Taker: An individual engaging in an assessment for purposes of earning a workforce skills credential. This term is used interchangeably with "candidate", "credential earner" and "employee."

## How is the Credentialing Security Framework organized?

The Credentialing Security Framework is comprised of six security areas. Each of these areas, described more fully below, has an impact on assessment security and the authentication and/or trustworthiness of credentials. Recognizing that security can vary considerably within each area, the Credentialing Security Framework rates each area on a level from .1 to .4, with .1 being the lowest level and .4 being the highest.

A. **Test Taker Identification**. Surrogate or proxy testing occurs when a registered test taker sends another person to test in his/her stead. From an exam security standpoint, identifying and, to the extent possible, authenticating the test taker is important to ensure test scores are attributed to, and credentials are issued to, the correct individual.
B. **Assessment Administration**. Ensuring standardized administration is a key to valid test scores. Accessing unauthorized testing aids, examinee copying, test material theft, and coaching examinees on responses are examples of activities that can result in invalid scores. Additional steps taken during the assessment administration can help to mitigate these risks.
C. **Secure Test Design**. Test design can either create or help reduce test security risks. Additional steps at the development and delivery stages can ensure testing materials are secure and appropriately protected from compromise. Retest parameters are associated with test design because of the relationship of item exposure to security; in other scenarios, retest parameters may be relevant to Investigation and Remediation determinations.
D. **Score Results Validation and Credential Authentication**. Invalid scores and fraudulent credentials erode trust in workforce skills credentials. Capabilities to detect and encourage reporting of score and credential concerns help reduce these risks.
E. **Investigation and Remediation**. If an exam security incident does occur, the ability to investigate and remediate issues can impact whether invalid scores or forged credentials are addressed and directly impacts the trustworthiness of the credential.
F. **Credential Sustainability**. Creating and maintaining processes that ensure the long term security health, value, and sustainability of a credential requires internal resources and regular financial investments.

For each area -- **Test Taker Identification, Assessment Administration**, **Secure Test Design**, **Score Results Validation and Credential Authentication**, **Investigation and Remediation,** and **Credential Sustainability**

-- the Credentialing Security Framework identifies the security elements anticipated in each level in terms that may be relevant to each stakeholder.

The **Level** column of each table identifies each level, from .1 to .4.

The **Test Taker/Credential User** column addresses both the test taker and credential user perspectives, as the interests of these stakeholders are generally aligned.

The **Simply Speaking** column provides, in less formal language, what occurs at each level; this section is focused primarily on the test taker. It is intended to help the credential earner and credential user understand in non-testing terms what actions will help ensure score validity and credential authenticity.

The **Test Publisher/Credential Issuer** column describes the elements at each level in greater specificity for use by credential issuers and test publishers.

On the following page is an abbreviated example of the details included in Levels .1 and .4 for the area of Test Taker Identification. By comparing these levels, a user of the Credentialing Security Framework can identify the difference in the degree of security associated with identification of a test taker, with Level .1 permitting self-identification and Level .4 containing more stringent identification capabilities.

## Example of Area A: Test Taker Identification

| Level | TEST TAKER / CREDENTIAL USER<br>Score validity and credential authenticity relies in part upon the following: | Simply Speaking: | TEST PUBLISHER / CREDENTIAL ISSUER<br>Score validity and credential authenticity relies in part upon the following: |
|---|---|---|---|
| .1 | • Examinee accurately self-identifies prior to starting the assessment<br>• Credential issuer may use other tools to confirm the examinee's identity | As a test taker, you need to honestly provide your identifying information to ensure the reported score and credential is given to the right person. The credential issuer may also use other tools to match your identity. | Minimal identification and authentication tools, such as<br>• Examinee self-identifies or is recognized by a test administrator or teacher as the registered test taker<br>• Credential issuer may seek to match identification through other tools (such as social media accounts or a learning management system (LMS))<br>• Credential issuer may seek to verify identification if questions arise |
| .4 | • Examinee accurately self-identifies prior to starting the assessment<br>• Examinee provides government-issued photo identification<br>• Examinee provides additional identification, such as a photograph, at the time of registration or prior to testing<br>• Examinee provides additional biometrics prior to and/or during testing<br>• Credential issuer has other procedures in place, such as data analytics, to address identification fraud | As a test taker, you need to honestly provide your identifying information as well as a government-issued photo identification at the time of testing. The credential issuer will also capture other information that can be used to match your identity. This helps ensure the reported score and credential is given to the right person and helps prevent cheating. | Strong identification and authentication tools, such as<br>• Examinee identification is established by requiring government-issued photo identification<br>• Examinee identification is further established via biometrics tools, challenge questions, and/or presentation of another form of photo identification<br>• Test taker image is captured at time of testing<br>• Credential issuer will seek to match identification through other tools and ensure duplicate account creation attempts are addressed<br>• Credential issuer will have hotline or webpage for reporting surrogate testing concerns to the issuer and will follow up on reports<br>• Credential issuer will use routinized method for identifying and addressing potential surrogate test takers |

## How can *Employers and other Credential Users* use the Credentialing Security Framework?

Entities and individuals that rely on authenticated and trustworthy credentials to make decisions (e.g., hiring, promotion, retention, fitness to practice, acceptance/admission into a program) can use the Credentialing Security Framework in several ways. First, they may use it to recognize and understand the exam security differences within the market. Second, they may request the Credentialing Security Framework Score for any given credential from a credential issuer or test publisher.

A credential issuer/test publisher should provide an overall Security Framework Score as well as individual levels for each area. The overall Security Framework Score can be calculated by adding the level subscores and dividing by 6. Thus, a credential issuer may represent its credential as having a Security Framework Score of .20, arrived at as follows:

**Sample Security Framework Score**

| Area | Level |
|---|---|
| A. Test Taker Identification | .1 |
| B. Assessment Administration | .2 |
| C. Secure Test Design | .3 |
| D. Score Results Validation and Credential Authentication | .2 |
| E. Investigation and Remediation | .2 |
| F. Sustainability | .2 |
| **Security Framework Score** (add each level and divide by **6**) | **.20** |

If the Credential Security Framework is used in connection with the Beta Connecting Credential Framework, a particular credential may possess a competency profile of 3 and a security level of .20, represented as 3.20.

Employers and other credential users can evaluate certain credentials to determine which credential(s) have a level of security commensurate with their needs and use that information to help inform which credential(s) they require or request from their employees or candidates.

## How can *Employees and other Credential Earners* use the Credentialing Security Framework?

An individual who seeks to attain a particular credential – whether for academic or workforce advancement or self-improvement – may also use the Credentialing Security Framework in a variety of ways. First, she can familiarize herself with the security levels available for credentials that may be of interest. Second, she may use the Credentialing Security Framework to evaluate whether the credentialing process is likely to result in credentials that are appropriately trustworthy and valuable for their intended use.

A credential issuer/test publisher should provide an overall Security Framework Score as well as levels for each area. Thus, a credential issuer may represent its credential as having a Security Framework Score of .23, arrived at as follows:

**Sample Security Framework Score**

| Area | Level |
|---|---|
| A. Test Taker Identification | .3 |
| B. Assessment Administration | .2 |
| C. Secure Test Design | .2 |
| D. Score Results Validation and Credential Authentication | .2 |
| E. Investigation and Remediation | .3 |
| F. Sustainability | .2 |
| **Security Framework Score** (add each level and divide by **6**) | **.23** |

As noted above, if the Security Framework Score is used in connection with the Beta Connecting Credential Framework, a credential may possess a competency profile of 3 and have a security level of .23, represented as 3.23.

Employees will be able evaluate whether particular credentials, both in terms of competencies measured and security levels, meet their personal growth and job objectives and use that information to help make decisions about which credential(s) they will pursue.

## How can *Credential Issuers and Test Publishers* use the Credentialing Security Framework?

A credential issuer or test publisher can use the Credentialing Security Framework to provide useful information concerning the exam security levels within each defined security area. In addition, it can evaluate its own assessment-based credentials and calculate a Security Framework Score. Evaluation should be based on whether the program meets the basic security elements demonstrated at each level. This evaluation will provide a credential issuer or test publisher with extremely useful information to assist in improving the security of its own credentials and credentialing systems. Finally, the issuer can use its Security Framework Score to provide additional information to clients and customers concerning the credential and appropriate use thereof. As an example of the information to be provided, a credential issuer may determine its credential has a Security Framework Score of .35, arrived at as follows:

**Sample Security Framework Score**

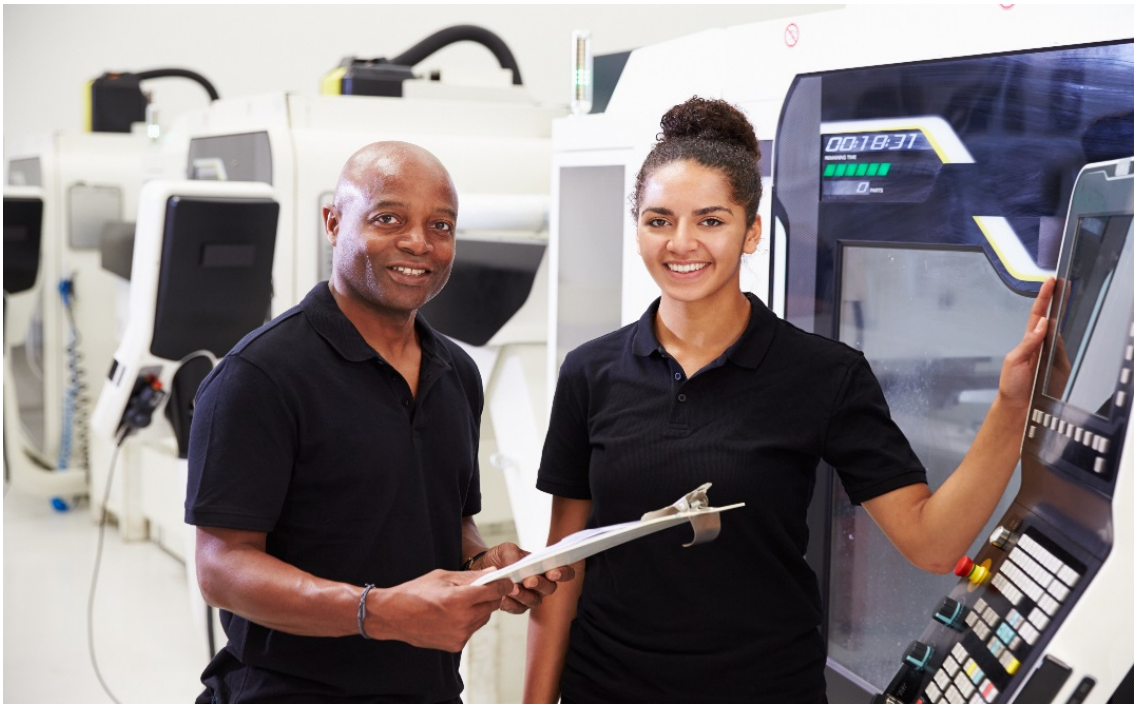
| Area | Level |
|---|---|
| 1. Test Taker Identification | .4 |
| 2. Assessment Administration | .4 |
| 3. Secure Test Design | .4 |
| 4. Score Results Validation and Credential Authentication | .2 |
| 5. Investigation and Remediation | .4 |
| 6. Sustainability | .3 |
| **Security Framework Score** (add each level and divide by **6**) | **.35** |

If the Secure Framework Score is used in connection with the Beta Connecting Credential Framework, a credential may be at competency profile 3 and have a security level of .35, represented as 3.35.

Identifying the security levels and Security Framework Score will enable credential issuers to improve understanding amongst various stakeholders and better meet market needs. Individuals, employers, and other credential users will be able to use the Credentialing Security Framework to assess a credential and determine whether both the competency measured and the security provided meet their unique needs.

## Questions and Next Steps

The Credentialing Security Framework is intended to bring greater clarity and transparency to the workforce skills credentialing market, inspiring greater trust in credentials and encouraging appropriate use of credentials. Stakeholders in the workforce credentialing ecosystem, including organizations such as Connecting Credentials, as well as credential issuers and test publishers, are invited to engage with the ATP to promote use of the Credentialing Security Framework. If there are questions concerning this Credentialing Security Framework, please email workforce@testpublishers.org. The ATP anticipates that as the market matures and technology evolves, this document will evolve as well, and a periodic review will be undertaken to ensure it remains current.



# Credentialing Security Framework

## Area A: Test Taker Identification

| Level | TEST TAKER / CREDENTIAL USER<br>Score validity and credential authenticity relies in part upon the following: | Simply Speaking: |
|---|---|---|
| .1 | • Examinee accurately self-identifies prior to starting the assessment<br>• Credential issuer may use other tools to confirm the examinee's identity | As a test taker, you need to honestly provide your identifying information to ensure the reported score and credential is given to the right person. The credential issuer may also use other tools to match your identity. |
| .2 | • Examinee accurately self-identifies prior to starting the assessment<br>• Examinee provides photo identification at the time of the assessment<br>• Credential issuer may use other tools to match the examinee's identity | As a test taker, you need to honestly provide your identifying information as well as a photo identification at the time of testing. This helps ensure the reported score and credential is given to the right person. The credential issuer may also use other tools to match your identity and to help prevent cheating. |
| .3 | • Examinee accurately self-identifies prior to starting the assessment<br>• Examinee provides government-issued photo identification<br>• Examinee provides additional identification, such as a photograph, at the time of registration or prior to testing | As a test taker, you need to honestly provide your identifying information as well as a government-issued photo identification at the time of testing. The credential issuer may also use other tools to match your identity and to prevent cheating. This helps ensure the reported score and credential is given to the right person. |
| .4 | • Examinee accurately self-identifies prior to starting the assessment<br>• Examinee provides government-issued photo identification<br>• Examinee provides additional identification, such as a photograph, at the time of registration or prior to testing<br>• Examinee provides additional biometrics prior to and/or during testing<br>• Credential issuer has other procedures in place, such as data analytics, to address identification fraud | As a test taker, you need to honestly provide your identifying information as well as a government-issued photo identification at the time of testing. The credential issuer will also capture other information that can be used to match your identity. This helps ensure the reported score and credential is given to the right person and helps prevent cheating. |

## Area A: Test Taker Identification

| Level | TEST PUBLISHER / CREDENTIAL ISSUER<br>Score validity and credential authenticity relies in part upon the following: |
|---|---|
| .1 | Minimal identification and authentication tools, such as<br>• Examinee self-identifies or is recognized by a test administrator or teacher as the registered test taker<br>• Credential issuer may seek to match identification through other tools (such as social media accounts or a learning management system (LMS))<br>• Credential issuer may seek to verify identification if questions arise |
| .2 | Moderate identification and authentication tools, such as<br>• Examinee provides photo identification to establish examinee identification<br>• Credential issuer may seek to match identification through other tools (such as social media accounts or an LMS)<br>• Credential issuer will seek to verify identification if questions arise |
| .3 | Moderate-strong identification and authentication tools, such as<br>• Examinee submits personal photo<br>• Examinee presents government-issued photo identification prior to testing to establish examinee identification; if online testing, a photo of the identification is also required<br>• Credential issuer may seek to match identification through other tools, such as biometrics or identification authentication software, and will ensure duplicate account creation attempts are addressed<br>• Credential issuer may have hotline or webpage for reporting surrogate testing concerns to the issuer and will follow-up on reports<br>• Credential issuer may use routinized method for identifying and addressing potential surrogate test takers |
| .4 | Strong identification and authentication tools, such as<br>• Examinee identification is established by requiring government-issued photo identification<br>• Examinee identification is further established via biometrics tools, challenge questions, and/or presentation of another form of photo identification<br>• Examinee image is captured at time of testing<br>• Credential issuer will seek to match identification through other tools and ensure duplicate account creation attempts are addressed<br>• Credential issuer will have hotline or webpage for reporting surrogate testing concerns to the issuer and will follow-up on reports<br>• Credential issuer will use routinized method for identifying and addressing potential surrogate test takers |

## Area B: Assessment Administration

| Level | TEST TAKER / CREDENTIAL USER<br>Score validity and credential authenticity relies in part upon the following: | Simply Speaking: |
|---|---|---|
| .1 | • Examinee has access to the rules prior to testing and has been told that abiding by any contract and following the assessment rules are important for valid outcomes<br>• Examinee can test in a non-controlled environment<br>• Examinee may or may not be observed during the exam | As a test taker, you are told or given the rules and are expected to follow them. If you do not, then the results may not be valid. |
| .2 | • Examinee has been provided the standardized rules in writing prior to testing<br>• Examinee has been told in writing that failure to follow the rules can result in consequences, including invalidating or failing to report scores or issue a credential<br>• Examinee must agree to test taker obligations and assessment rules prior to testing<br>• Examinee must test in a semi-controlled and distraction-free environment<br>• Examinee will be observed during the test to help ensure adherence to testing rules<br>• Steps are taken to deter or detect cheating, such as prohibiting use of notes or other materials that can provide an unfair advantage during testing | As a test taker, you can review the rules and are expected to follow them. If you do not, then the assessment results may not be valid. There are consequences for failing to follow the rules. You must agree to the rules and the consequences before you can test. Test staff will also observe you during testing to ensure the rules are followed. |
| .3 | • Examinee has been provided standardized testing rules in writing prior to testing<br>• Examinee has been told in writing that failure to follow the rules can result in consequences, including invalidating or failing to report scores or issue a credential<br>• Examinee must agree to test taker obligations and assessment rules prior to testing<br>• Examinee must test in a distraction-free environment<br>• Examinee will be observed by at least one trained professional during the test to help ensure adherence to testing rules<br>• Steps are taken to deter or detect cheating<br>• The test site or proctor will be audited if questions arise regarding following testing rules | As a test taker, you will receive the rules and are expected to follow them. If you do not, then the results may not be valid. There are consequences for failing to follow the rules. You must agree to the rules and the consequences before you can test. Your test will be held in a distraction-free environment, and test staff will observe you during testing to ensure the rules are followed. |

(level .4 appears on page 24)

## Area B: Assessment Administration

| Level | TEST PUBLISHER / CREDENTIAL ISSUER<br>Score validity and credential authenticity relies in part upon the following: |
|---|---|
| .1 | Minimal standardized administration procedures, such as<br>• Testing rules are provided to examinee in advance of testing<br>• Test may be self-administered by examinee<br>• Test content is accessed by the examinee with minimal security protocols<br>• May or may not include live or online proctoring |
| .2 | Moderate standardized administration procedures, such as<br>• Defined and written secure data and exam distribution and storage procedures<br>• Secure physical testing room layout is documented and communicated to test staff<br>• Chain of custody documentation/access control and logging is expected<br>• Minimal consequences for rules violations<br>• Rules and consequences for violating them are communicated to examinee in advance of testing<br>• Rules and consequences for violating them are publicly available<br>• Written assessment administration policies and procedures are communicated to test staff no later than time of testing<br>• Live or online proctoring is provided throughout testing, typically by proctor with no or minimal training<br>• Entity or individual administering tests is responsible for implementation of assessment administration policies and procedures (i.e., credential issuer is responsible for establishing the assessment administration requirements, but the organization administering tests is responsible for implementation with little oversight from credential issuer)<br>• Credential issuer offers some training of test staff regarding administration policies and procedures |
| .3 | Moderate-strong standardized administration procedures, such as<br>• Defined and written secure data and exam distribution and storage procedures<br>• Secure physical testing room layout is documented and communicated to test staff, and seating chart or testing device is recorded<br>• Chain of custody documentation/access control, logging, and monitoring is expected<br>• Rules and consequences for violating them are communicated and agreed to by examinee<br>• Rules and consequences for violating them are publicly available<br>• Written assessment administration policies and procedures are communicated to test staff in advance of testing<br>• Live proctoring at secure test site, which may or may not be under the control of the publisher/issuer or its vendors<br>• Routinized collection and analysis of administration documentation, including irregularity reports<br>• Entity administering tests is responsible for implementation of assessment administration policies and procedures<br>• Ad hoc audit of assessment administrations<br>• Credential issuer conducts some mandatory training of test staff regarding administration policies and procedures prior to test staff's first administration |

(level .4 appears on page 25)

## Area B: Assessment Administration

| Level | TEST TAKER / CREDENTIAL USER<br>Score validity and credential authenticity relies in part upon the following: | Simply Speaking: |
|---|---|---|
| .4 | • Examinee has been provided standardized testing rules in writing prior to testing<br>• Examinee has been told in writing that failure to follow the rules can result in consequences, including invalidating or failing to report scores or issue a credential<br>• Examinee must agree to test taker obligations and assessment rules prior to testing<br>• Examinee must test in a designated, strictly controlled, and distraction-free environment<br>• Examinee will be observed by at least one highly trained professional during the test to help ensure adherence to testing rules<br>• Steps are taken to deter or detect cheating<br>• The test site or proctor will be audited if questions arise regarding following testing rules | As a test taker, you will receive the rules and are expected to follow them. If you do not, then the results may not be valid. There are consequences for failing to follow the rules. You must agree to the rules and the consequences before you can test. Your test will be held in a strictly controlled and distraction-free environment. Trained test staff will observe you during testing to ensure the rules are followed. The credential issuer will take additional steps to make sure that testing rules are followed. |

## Area B: Assessment Administration

| Level | TEST PUBLISHER / CREDENTIAL ISSUER<br>Score validity and credential authenticity relies in part upon the following: |
|---|---|
| .4 | Strong standardized administration requirements, such as<br>• Defined and written secure data or exam distribution and storage requirements<br>• Defined physical testing room layout requirements for establishing secure, controlled test environments, and seating chart or testing device is recorded<br>• Rules and consequences for violating them are communicated and agreed to by examinee<br>• Rules and consequences for violating them are publicly available<br>• Written assessment administration policies and procedures are communicated to test staff in advance of testing<br>• Live proctoring at secure test site that is under strict control of publisher/issuer or its agents and vendors<br>• Required chain of custody documentation/access control and logging<br>• Routinized collection and analysis of administration documentation, including irregularity reports<br>• Use of technology to identify or block use of unauthorized digital devices<br>• Regular auditing of administrations<br>• The organization that issues the credential is responsible for ensuring adherence to test security and assessment administration requirements and score validation<br>• Credential issuer conducts annual mandatory training of certified test staff regarding administration policies and procedures |

## Area C: Secure Test Design

| Level | TEST TAKER / CREDENTIAL USER<br>Score validity and credential authenticity relies in part upon the following: | Simply Speaking: |
|---|---|---|
| .1 | • Examinees are expected to follow retest guidelines | As a test taker, if you want to take the test again, you should follow any guidelines for retesting recommended by the credential issuer so the results are accurate. |
| .2 | • Test questions are periodically replenished and rotated<br>• Rules are in place to help avoid examinees seeing all of the same test questions if the examinees test more than one time | As a test taker, if you want to take the test again, you should follow the written guidelines for retests recommended by the credential issuer so the results are accurate. |
| .3 | • Test questions are protected and are replaced and rotated on a regular basis<br>• There are rules and procedures in place to ensure examinees do not see the same test questions if they test more than one time | As a test taker, if you want to take the test again, you should follow the written and enforced guidelines for retests recommended by the credential issuer so the results are accurate. Test questions are protected, and you may be tested with different types of test questions to protect the test questions and answers from theft. |
| .4 | • Test questions are highly protected and are replaced and rotated on a frequent basis.<br>• There are rules and rigorous procedures in place to help ensure examinees do not see the same test questions if they test more than one time | As a test taker, if you want to take the test again, you must follow the written and enforced guidelines for retests provided by the credential issuer so the results are accurate. Test questions are highly protected, and it is likely you will be tested with different types of test questions to protect the test questions and answers from theft. |

## Area C: Secure Test Design

| Level | TEST PUBLISHER / CREDENTIAL ISSUER<br>Score validity and credential authenticity relies in part upon the following: |
|---|---|
| .1 | Minimal form/item rotation and retest rules, such as<br>• Minimal item development/replenishment/rotation/retirement schedule with periodic replenishment<br>• Access to items, forms, and rotation information is controlled and logged<br>• No retest restrictions, although recommendations may be documented |
| .2 | Moderate form/item rotation and retest rules, such as<br>• Moderate item development/replenishment/rotation/retirement schedule with periodic replenishment<br>• Access to items, forms, and rotation information is controlled and logged<br>• Recommended retest policies provided in writing |
| .3 | Moderate-strong form/item rotation and retest rules, such as<br>• Written and defined item development/replenishment/rotation/retirement schedule with periodic replenishment<br>• Access to items, forms, and rotation information is highly controlled, logged, and monitored<br>• Documented and enforced retest requirements<br>• Registration and system capabilities are in place to identify retesting and to rotate form assignment; test may be delivered in Computer Adaptive Testing (CAT) or Linear on the Fly Testing (LOFT) format<br>• Test may also include secure questions and other capabilities to capture data that may be used for analytics (such as identification, timing, and watermarks) |
| .4 | Strong form/item rotation and retest rules, such as<br>• Written and defined item development/replenishment/rotation/retirement schedule with frequent replenishment<br>• Access to items, forms, and rotation information highly is controlled, logged, and monitored<br>• Documented, enforced, and routinely audited retest requirements<br>• Registration and system capabilities are in place to identify retesting and to rotate form and item assignment; test may also be delivered in more protective formats such as CAT or LOFT<br>• Test will also include secure questions and other capabilities to capture data that may be used for analytics (such as identification, timing, and watermarks) |

## Area D: Score Results Validation and Credential Authentication

| Level | TEST TAKER / CREDENTIAL USER<br>Score validity and credential authenticity relies in part upon the following: | Simply Speaking: |
|---|---|---|
| .1 | • If the examinee follows the testing rules and passes the exam, the credential can be generated by the test taker | As a test taker, if you follow the rules and pass the test, you can generate the credential yourself. |
| .2 | • If the examinee follows the rules and passes the exam, the credential is generated by the entity administering the exam, such as an employer or workforce agency<br>• Tools are available, such as hotlines, for individuals to raise concerns about cheating or score validity<br>• Rule violations or validity concerns may be investigated<br>• Scores may be cancelled or credentials revoked if appropriate | If you pass the exam, then the place you took the test is responsible for generating your credential. If someone has a question about whether the credential is valid, there are tip lines or other tools available to report concerns. Those concerns may be investigated and if cheating or other validity issues are discovered, then the credential may be revoked. |
| .3 | • If the examinee follows the rules and passes the exam, the credential is generated by the credential issuer or its vendor<br>• Credentials can be authenticated by various means<br>• Tools are available, such as hotlines, for individuals to raise concerns about score validity<br>• Rule violations or validity concerns may be investigated<br>• Scores may be cancelled or credentials revoked if appropriate | If you pass the exam, then the credential issuer will provide your credential to you. The credential will be protected from copying. If someone has a question about whether the credential is valid, there are tools available to report those concerns. Concerns may be investigated and if cheating or other validity issues are discovered, then the credential may be revoked. |
| .4 | • If the examinee follows the rules and passes the exam, the credential is generated by the credential issuer or its vendor<br>• Credentials can be authenticated by multiple means<br>• Tools are available, such as hotlines, for individuals to raise concerns about score validity<br>• Rule violations or validity concerns are investigated<br>• Scores will be cancelled or credentials revoked if appropriate | If you pass the exam, then the credential issuer will provide your credential to you. The credential will be protected from copying. If someone has a question about whether the credential is valid, there are tools available to report those concerns. Concerns are investigated and if cheating or other validity issues are discovered, then the credential will be revoked. |

## Area D: Score Results Validation and Credential Authentication

| Level | TEST PUBLISHER / CREDENTIAL ISSUER<br>Score validity and credential authenticity relies in part upon the following: |
|---|---|
| .1 | Minimal credential validation methods, such as<br>• Credentials can be self-generated by the test taker based on test results<br>• Credentials are branded |
| .2 | Moderate credential validation methods, such as<br>• Credentials are generated by entity administering the test, such as an employer or workforce agency<br>• Credentials are uniquely branded<br>• Hotline is available for raising questions or reporting concerns<br>• Credential issuer or test publisher may investigate and may cancel scores or revoke credential if appropriate |
| .3 | Moderate-high credential validation methods, such as<br>• Credentials are issued by credentialing organization or its vendor<br>• Credentials are protected via watermark or other security tool from easy replication<br>• Credential issuer may have hotline or webpage for reporting authentication concerns<br>• Credentials can be authenticated by credential users and authorized individuals<br>• Credential issuer or test publisher may investigate and may cancel scores or revoke credential if appropriate |
| .4 | Strong credential validation methods, such as<br>• Credentials are issued by credentialing organization or its vendor<br>• Credentials contain more than one security tool to prevent forgeries or spoofs<br>• Credential issuer has user-friendly credential authentication mechanisms that make it easy for credential users to authenticate a credential<br>• Credential issuer has hotline or other tools available for individuals to raise authentication concerns<br>• Credential issuer or test publisher routinely investigates and will cancel scores or revoke credential if appropriate |

## Area E: Investigation and Remediation

| Level | TEST TAKER / CREDENTIAL USER<br>Score validity and credential authenticity relies in part upon the following: | Simply Speaking: |
|---|---|---|
| .1 | • Examinees are provided rules that state what is expected of them before, during, and after testing<br>• If concerns are raised about rules violations or intellectual property violations, concerns may be investigated and some action may be taken | As a test taker, you will be given information about the rules you are expected to follow before, during, and after testing. If concerns are raised about whether you followed the rules, those concerns may be investigated. |
| .2 | • Examinees are provided rules that state what is expected of them before, during, and after testing<br>• Dedicated methods for raising score review or credential authenticity concerns are in place<br>• If concerns are raised about rules violations or intellectual property violations, concerns may be investigated and some action may be taken | As a test taker, you will be given information about the rules you are expected to follow before, during, and after testing. If you or others have concerns about whether the rules have been followed, a hotline or other tools are available to raise those concerns. Concerns may be investigated and the credential issuer can revoke your credential. |
| .3 | • Examinees are provided rules that state what is expected of them before, during, and after testing<br>• Dedicated methods for raising score review or credential authenticity concerns are in place<br>• If concerns are raised or identified about rules violations or intellectual property violations, they are investigated<br>• Rules violations and invalid scores are redressed, including cancellation and notification to a credential recipient | As a test taker, you will be given information about the rules you are expected to follow before, during, and after testing. If you or others have concerns about whether the rules have been followed, a hotline or other tools are available to raise those concerns. The credential issuer may also independently identify concerns. Concerns will be investigated and the credential issuer can revoke your credential. |
| .4 | • Examinees are provided rules that state what is expected of them before, during, and after testing<br>• Dedicated methods for raising score review or credential authenticity concerns are in place<br>• The credential issuer routinely monitors to ensure score validity and intellectual property protection<br>• If concerns are raised or identified about rules violations or intellectual property violations, they are investigated<br>• Rules violations and invalid scores are redressed, including cancellation and notification to a credential recipient | As a test taker, you will be given information about the rules you are expected to follow before, during, and after testing. If you or others have concerns about whether the rules have been followed, a hotline or other tools are available to raise those concerns. The credential issuer will also independently identify concerns. Concerns will be investigated and the credential issuer can revoke your credential. An employer may be notified if a credential is revoked. |

## Area E: Investigation and Remediation

| Level | TEST PUBLISHER / CREDENTIAL ISSUER<br>Score validity and credential authenticity relies in part upon the following: |
|---|---|
| .1 | Limited detection, investigation, and remediation capabilities, such as<br>• Limited investigation into suspect score or credential validity; may be investigation into intellectual property concerns<br>• Limited processes for investigation and remediation<br>• May be some messaging to examinees and third parties regarding how to raise questions or concerns |
| .2 | Minimal detection, investigation, and remediation capabilities, such as<br>• Credential issuer has some capabilities in place that can be used to report test security concerns<br>• Credential issuer has data analysis tools that are utilized if a concern arises<br>• Credential issuer has processes to investigate and remediate test security issues<br>• Credential issuer has right to notify individuals and credential users if there is a concern about validity of scores or authentication of a credential |
| .3 | Moderate detection, investigation, and remediation capabilities, such as<br>• Credential issuer has general hotline capabilities to enable reporting of test security concerns<br>• Credential issuer has data analysis tools that are used to detect and/or investigate concerns<br>• Credential issuer periodically uses web and social media monitoring to identify and investigate test security concerns<br>• Credential issuer has established processes to investigate and remediate test security issues and does, in fact, do so<br>• Credential issuer has right to cancel results/revoke credential and to notify credential recipients of cancellation/revocation, and does, in fact, cancel and notify when appropriate |
| .4 | Strong detection, investigation, and remediation capabilities, such as<br>• Credential issuer has dedicated security hotline capabilities to enable anonymous reporting of test security concerns<br>• Credential issuer uses routinized data analysis tools to proactively identify and investigate security concerns<br>• Credential issuer routinely and regularly uses web and social media monitoring to proactively identify and investigate test security concerns<br>• Credential issuer has established processes to investigate and remediate test security issues and does, in fact, do so on a regular basis<br>• Credential issuer has right to cancel results/revoke credential and to notify credential recipients of cancellation/revocation, and does, in fact, cancel and notify when appropriate |

## Area F: Credential Sustainability

| Level | TEST TAKER / CREDENTIAL USER<br>Score validity and credential authenticity relies in part upon the following: | Simply Speaking: |
|---|---|---|
| .1 | • Examinee is provided information regarding testing rules<br>• Credential users are provided information about appropriate credential use | As a test taker, you will be given some information about appropriate testing rules, and you will be put on notice regarding copyrights. |
| .2 | • Examinee is provided information regarding testing rules<br>• Test administrators receive some written procedures related to test security<br>• Credential users are provided information about appropriate credential use<br>• The credential issuer takes some steps to protect the value of the credential over time | As a test taker, you will be given information about appropriate testing rules, and you will be put on notice regarding copyrights. The credential issuer takes some steps to ensure the ongoing trustworthiness of the credential. |
| .3 | • Examinee is provided information regarding testing rules<br>• Test administrators receive some written procedures related to test security<br>• Credential users are provided information about appropriate credential use<br>• The credential issuer takes steps to protect the value of the credential over time<br>• The credential issuer takes some steps to audit assessment administrations | As a test taker, you will be given information about appropriate testing rules, and you will be put on notice regarding copyrights. The credential issuer takes steps to ensure the ongoing trustworthiness of the credential. |
| .4 | • Examinee is provided information regarding testing rules<br>• Test administrators receive some written procedures related to test security<br>• Credential users are provided information about appropriate credential use<br>• The credential issuer takes steps to protect the value of the credential over time<br>• The credential issuer regularly audits assessment administrations<br>• Credential issuer has annual audit, clear internal responsibility for ensuring score validity, and separate and sufficient budget to protect exam results and credentials issued | As a test taker, you will be given information about appropriate testing rules, and you will be put on notice regarding copyrights. The credential issuer takes significant steps to ensure the ongoing trustworthiness of the credential. |

## Area F: Credential Sustainability

| Level | TEST PUBLISHER / CREDENTIAL ISSUER<br>Score validity and credential authenticity relies in part upon the following: |
|---|---|
| .1 | Minimal program sustainability practices, such as<br>• Credential issuer has minimal documentation and support related to test security<br>• Minimal documented policies or processes and some training provided to credential issuer's staff<br>• Credential issuer communicates testing rules and appropriate credential use<br>• Credential issuer may note copyright on testing materials |
| .2 | Moderate program sustainability practices, such as<br>• Credential issuer has documented procedures and policies related to test security and incident response<br>• Documented security plan with a test security role identified at a minimum, and some training provided to credential issuer's staff<br>• Credential issuer communicates testing rules and appropriate credential use<br>• Credential issuer notes copyright on testing materials<br>• Credential issuer may have documented credential expiration/renewal policies |
| .3 | Moderate-strong program sustainability practices, such as<br>• Credential issuer conducts annual internal test security review and has documented procedures and policies related to test security and incident response<br>• Documented security plan with some roles and responsibilities identified, and some training provided to credential issuer's staff<br>• Credential issuer communicates testing rules and appropriate credential use<br>• Credential issuer registers and conspicuously notes copyright on testing materials<br>• People resources are assigned to address test security needs<br>• Credential issuer has a separate and adequate budget and contingency fund for test security<br>• Credential issuer conducts ad hoc audits of assessment administrations<br>• Credential issuer has documented credential expiration/renewal policies and may note such dates, if any, on or in association with the credential |
| .4 | Strong program sustainability practices, such as<br>• Organization issuing credential conducts annual internal test security review and has documented procedures and policies related to test security and incident response<br>• Documented security plan with roles and responsibilities for test security and regular training provided to credential issuer's staff<br>• Credential issuer communicates testing rules and appropriate credential use<br>• Credential issuer conspicuously notes copyright on testing materials<br>• Credential issuer has assigned and adequate people resources to proactively and reactively address test security needs<br>• Credential issuer has a separate and adequate annual budget and contingency fund for test security<br>• Credential issuer conducts regular audits of assessment administrations<br>• Credential issuer has documented credential expiration/renewal policies and clearly notes such dates, if any, on or in association with the credential |

# References:


http://connectingcredentials.org, accessed February 3, 2017.

http://connectingcredentials.org/wp-content/uploads/2015/06/MakingTheCase-6-8-15.pdf, accessed February 3, 2017.

http://connectingcredentials.org/framework/, accessed February 3, 2017.

http://ec.europa.eu/education/policy/school_en, accessed February 3, 2017.

http://keyconet.eun.org/eu-policy, accessed February 3, 2017.

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:394:0010:0018:EN:PDF, accessed February 3, 2017.

Association of Test Publishers / National College Testing Association (2015). *Proctoring Best Practices*.

Association of Test Publishers/ Workforce Skills Credentialing Division (2017). *Workforce Skills Credentialing Security Survey Report.*

Wollack, J. A. & Fremer, J. J. (Eds.) (2013). *Handbook of Test Security*. New York, NY: Routledge.