WHITE PAPER

Credentialing Cybersecurity Workforce

CompTIA INSIGHTS INTO
THE CERTIFICATION PROCESS

CompTIA

Table of Contents

3 Foreword
4 The Cybersecurity Training Imperative
5 Industry-Driven, Vendor-Neutral Certifications: The CompTIA Story
6 IT Certification in the Cybersecurity Environment
What is a Certification?
7 Producing Trusted Cybersecurity Certifications
The Certification Development Process
How is an IT Certification Made?
9 How is a Certification Delivered?
10 What to Measure in a Credential Examination: Knowledge, Performance or Both?
11 The CompTIA Public-Private-Academic Partnership: Optimum Responsiveness to Rapid Developments in the Cybersecurity Threat Environment
13 CompTIA and the Cybersecurity Credentials Industry
13 Glossary
17 Appendices

Foreword

CompTIA, the leading global provider of vendor-neutral IT certifications, develops security certifications that are foundational and promote the workforce skills needed to combat cyber threats and weaknesses. This white paper provides a transparent explanation of CompTIA's expertise in developing, disseminating, and updating IT security certifications. Although other peer organizations may offer procedural variations, it is our hope that this description of the CompTIA methodology will provide a broader understanding of the importance and effectiveness of the private sector credentialing community. In this paper we set forth:

- The importance of developing varied career paths to meet today's workforce and cybersecurity challenges.
- CompTIA's network of learning and testing partners and the origin and importance of vendor-neutral certifications.
- The meaning of a certification: A credential achieved through examination that validates the knowledge and skills of an individual or organization.
- How effective certification is constructed and kept up to date by assembling subject matter experts to develop a Job Task Analysis (JTA), an examination blueprint, and extensive examination questions that map to the blueprint.
- A discussion of our testing partners and the steps undertaken to ensure the integrity of examinations and their results.
- The value of both knowledge- and performance-based testing.
- The breadth of CompTIA relationships with government and academic communities, all of which enhance the effectiveness of the credential and the rapidity by which real-world developments can drive updates, improvements, and training.
- A framework that demonstrates order and coherence to the cybersecurity credentialing ecosystem.

With a rapidly developing cybersecurity threat matrix, both government and private-sector professionals must be nimble and collaborative. We are all a part of the solution.

Todd Thibodeaux, President and CEO
CompTIA

The Cybersecurity Training Imperative

Technology innovation has given us an interconnected global marketplace. We now have hundreds of millions of online users with constantly evolving mobile computing platforms offering ubiquitous access to information, communication, and commerce wherever we live. We now have more raw computing power contained in smart phones than the cumulative mission-control IT capability that propelled mankind on the first lunar missions in the 1970s. The correspondingly complex and mobile nature of digital threats to the world's computer networks is growing at the same exponential pace.

Training the cybersecurity workforce for tomorrow's threat environment requires forward-looking approaches; merely informing end users and IT security professionals about existing cyber threats is not enough. Those responsible for hiring the best human cybersecurity talent must have confidence—before a breach or breakdown occurs—that employees are trained and equipped in a manner that can be confidently identified, measured, and validated. The challenge we face is to produce the best-trained professionals in the world, equipped with proper tools. Further, it is essential to develop and provide ongoing training so that the professional workforce is prepared to address new and emerging threats to our increasingly digital way of life.

Cybersecurity professionals rely on a variety of tools to prepare for defending against and responding to cyber threats. In most cases, training and corresponding credentials come through degree programs (from higher education or technical training institutions) and technical certifications (in either vendor-specific software or hardware products). Other sources include vendor-neutral credentials that address a broader subject or practice area, on-the-job training programs, internships or other practical, experience-based programs.

In the cybersecurity world, career paths vary from technical information assurance and auditing to IT management—with levels within each scaling from apprentice to master. Each pathway serves a distinct and important role in addressing today's cyber threats and requires unique training and skill sets.[1] (See Appendix 1 for details.)

CompTIA certifications also cover a wide array of IT fields including cloud, mobility, storage, healthcare, green IT, and more. However, the focus of this paper is the suite of IT certifications that are the basis for cybersecurity training and the specific role of certifications in addressing the critical need to train, credential, and deploy thousands of professionals to protect our national IT infrastructure.

1. A useful resource for viewing the structure for how IT certifications advance along different career paths is the Department of Defense Directive 8570 (http://www.dtic.mil/whs/directives/corres/pdf/857001p.pdf). Civilian career paths can and do map to DOD equivalents. Another resource is the Essential Body of Knowledge matrix developed by the Department of Homeland Security (http://www.us-cert.gov/ITSecurityEBK/EBK%20Matrix-Sept08.pdf).

> "No foreign nation, no hacker, should be able to shut down our networks, steal our trade secrets, or invade the privacy of American families, especially our kids. We are making sure our government integrates intelligence to combat cyber threats, just as we have done to combat terrorism. And tonight, I urge this Congress to finally pass the legislation we need to better meet the evolving threat of cyber-attacks, combat identity theft, and protect our children's information. If we don't act, we'll leave our nation and our economy vulnerable. If we do, we can continue to protect the technologies that have unleashed untold opportunities for people around the globe."
>
> – President Barack Obama, State of the Union Address, January 2015

Industry-Driven, Vendor-Neutral Certifications: The CompTIA Story

The success of the personal computer led the computer service and repair industries to commission CompTIA to create its globally recognized, vendor-neutral CompTIA A+ certification program in 1992, which has been continually updated in the over two decades since. The continuing success of CompTIA's A+ certification demonstrates an ongoing need to provide a means of validating skills across a wide spectrum of computer hardware and software. Following on the success of the CompTIA A+ certification, CompTIA developed and introduced CompTIA Network+, and CompTIA Security+. Each CompTIA certification is industry- driven, validating technical skills for both individuals working in IT and for the people who hire and train them.

By securing and validating core skills and knowledge, both job-seekers and established professionals can progress to more complex and specialized cybersecurity credentials, such as vendor-specific hardware and software training. As a career in cybersecurity matures, it may well necessitate higher-level, specialty training and skills in subjects such as security auditing, forensics, and cybersecurity management. Workers might also feel compelled to acquire additional credentials to validate those skills to current or prospective management. A diverse array of career paths needs to be available in order to maintain a skilled cybersecurity workforce.

Along with a global network of third-party academic and training providers, CompTIA plays an important role in the skills-development efforts for today's cybersecurity workforce. As a result of our focus on creating independent certification credentials developed in isolation from the training community, CompTIA is recognized worldwide as a trusted provider of vendor-neutral certification exams.

IT Certification In The Cybersecurity Environment

In addition to validating core competencies, certifications can be developed and deployed quickly to address ever-evolving threats to our IT infrastructure. Certifications can demonstrate that a workforce remains current and informed on technology advancements that defend against ever-present cyber threats.

CompTIA has put an increasing focus on cybersecurity, enabling professionals and solution providers with foundational principles for securing a network and managing risk. The responsiveness of CompTIA's credentialed certifications in addressing technological advancements has led to private sector and government mandates for continuing education requirements for cybersecurity professionals—a development that CompTIA fully supports.

WHAT IS A CERTIFICATION?

Determining what constitutes a certification as compared to a certificate, a credential, and accreditation can be challenging. Put simply, a certification is achieved through an examination that validates the knowledge and/or skills of an individual or an organization. A certification differs from a certificate program, which is usually an educational offering that confers a document at the program's conclusion. The American National Standards Institute (ANSI) provides a useful definition:

Certification and certificate are distinct terms, yet they are often used synonymously. Certification is more comprehensive and includes an assessment of an individual's knowledge, skills, and abilities based on a body of knowledge pertaining to a profession or occupation.

In comparison, certificate programs emphasize learning events and coursework completion. Certification is valid for a specific time period and involves recertification at the expiry of the stated period. Certificates are generally issued for life.[2]

Beyond this important distinction, the industry often refers to credentials and accreditations. Credentials attest to someone's knowledge or authority such as a FBI agent badge, a Ph.D. in physics, or an IT security certification. Accreditation is granted when stated quality criteria are met. For example, by submitting to a voluntary, self-regulatory process through American National Standards Institute (ANSI), CompTIA has sought accreditation of foundational certifications CompTIA A+, Network+ and Security+, as well as the CompTIA Advanced Security Practitioner certification.

The wide variety of methods used to train and validate knowledge for cybersecurity professionals demonstrates there is no "one-size-fits-all" solution. While most academic and professional programs promote broad, introductory knowledge for cybersecurity professionals, the generalized scope of such programs is impractical for many full-time IT professionals. Specialty certifications can be more effective in providing "just-in- time" training and validation for a specific technology tool or skill. But in some situations, more in-depth training and certification, which generally requires more experience in a profession and more core knowledge, is appropriate. Ideally, IT professionals, along with their career guidance personnel, can construct learning and career paths using a variety of credentialing options as tools to develop the skill sets required.

2. https://www.ansica.org/wwwversion2/outside/PERfaq.asp?menuID=2

Producing Trusted Cybersecurity Certifications

IT certification has evolved into a validation instrument that is a trusted resource in both the IT and the human resources (HR) communities. How is an internationally validated and trusted certification instrument constructed?

THE CERTIFICATION DEVELOPMENT PROCESS

To be an effective and defensible IT certification, a credential must meet the following criteria:

- **Technical Precision and Accuracy** with respect to the current and particular body of knowledge.
- **Comprehensive in Scope** to validate the breadth of skills required by the IT and cybersecurity professional.
- **Educationally Valid Verification** to fairly and accurately gauge skills and knowledge.
- **Integrity in the Exam Creation Process** so students trust that an exam fairly validates the requisite skills for a particular job or skills area and is worth requisite study and experience; and that IT management and HR professionals trust both the credential and the holder as a person who possesses genuine and comprehensive knowledge.
- **Rigorous and Effective Security in Delivery** to ensure that cheating does not take place.

To meet these important benchmarks, CompTIA employs an exacting process to develop and disseminate credentials.

HOW IS AN IT CERTIFICATION MADE?

Development of an IT certification begins by identifying and bringing together Subject Matter Experts (SMEs) to draft a blueprint for the examination known as a Job Task Analysis (JTA). Using the JTA, SMEs proceed to draft a series of questions that form the basis of the certification exam. (See Appendix 2.)

Bringing Subject Matter Experts to the Table

To be accurate and to validate current knowledge, CompTIA first selects SMEs to construct a certification instrument. Each SME is required to sign a legally binding non-disclosure agreement[3] precluding any profit motive in the credentials-training industry. This is done to address any potential conflicts of interest. To assure both a balanced and comprehensive product, SMEs are selected from a wide variety of disciplines and vertical markets — including government, private sector, and, where individuals are not in any way involved in course preparation or delivery for IT certifications, academic professions. Recent SMEs for CompTIA IT security certifications have included government professionals from the U.S. Department of Homeland Security, the U.S. Air Force, and the U.S. Navy. Private-sector experts from companies including Booz Allen Hamilton and Lockheed Martin have also participated. CompTIA allows no more than two individuals from the same organization or agency to participate in the process, ensuring that the exam is not skewed or biased toward any one agency or vendor technology.

3. For details about the requirements SMEs must meet before participating in CompTIA's certification development process, see http://certification.comptia.org/get-involved/examdevelopment.aspx

After a group of qualified SMEs is selected, it is sequestered at CompTIA's headquarters (much like a deliberating jury in a legal setting) with precautions taken against tampering or outside influences upon the group's deliberations.

Creating a Job Task Analysis and Examination Blueprint

The foundation of a strong certification program is a JTA that defines the subject matter content that is valid for assessment. The JTA is then used to develop a blueprint to test against. The JTA, along with other test development procedures, helps ensure the defensibility of the resulting content. The collaborative nature of the process is underscored in the requirement that both the draft JTA and the draft examination blueprint cannot be received in final form until a significant volume of feedback is received from qualified professionals worldwide.[4] The partnership between public, private, and academic sectors of the cybersecurity learning, research, and practice domains is clearly evident in the final product.

The Separation of Teaching and Learning Materials from Test Creation

Once the JTA and examination blueprint are published, a number of activities take place. Curriculum developers, book publishers, authors and designers, and other professionals begin developing teaching and learning materials for training and the eventual certification exam.

Certification candidates have access to resources like these as well as resources like CompTIA CertMaster. CompTIA CertMaster is an online study companion using four components to ensure professionals not only learn but retain the information they are studying. These four components include brain science, adaptive learning, superlative study tools, and mobile learning.

When it comes to certification exam integrity, CompTIA has maintained a policy of precluding all instructors, professors, authors, training executives, and even unauthorized members from their own organization (e.g., marketing and sales personnel) from the vital activities required in the creation of an examination. While there may be other avenues to a similar outcome, this process protects against proprietary knowledge obtained in the creation of a test from being used to "teach to the test." CompTIA's practice is to maintain a clear wall of separation to protect the integrity and validity of the examination process.

Writing the Questions

Once the JTA and examination blueprint are completed another group of SMEs is convened for the question writing phase of the process. This is a difficult and precise process, because hundreds of questions are needed for the initial drafts of the exam. Questions are accepted based on their relevance to the material and the clarity of the question, with care to omit any ambiguities in terminology or verbiage.

Once the required number of questions mapped to every area on the examination blueprint is created, the examination—still in beta format—is published. At authorized CompTIA testing centers, professionals are encouraged to take the beta examination and submit feedback. After the beta exam is completed, a standard-setting workshop is conducted to determine that valid inferences are made from the test. This is one of the most crucial steps in exam development. At the workshop, another group of SMEs estimates the number of minimally qualified candidates who would answer each question correctly. As such, the workshop determines the cut score, which is the demarcation between pass and fail.

4. CompTIA generally seeks approximately 200 responses within the target audience in order to validate a JTA blueprint.

"With this increased reliance on cyber-dependent systems, come increased threats and vulnerabilities. Protecting the cybersecurity of our critical infrastructure is a top priority for the nation, and in February 2013 the President signed Executive Order (EO) 13636: Improving Critical Infrastructure Cybersecurity and released Presidential Policy Directive (PPD)-21: Critical Infrastructure Security and Resilience, which aims to increase the overall resilience of U.S. critical infrastructure."

– About the Critical Infrastructure Cyber Community C³ Voluntary Program, Dept. of Homeland Security; 2013

Keeping the Credential Current, Valid, and Relevant

Given the type of threats and the corresponding levels of complexity of hardware and software to meet the exigencies of IT security, a valid certification examination must stay up to date.

CompTIA relies upon a Certification Advisory Committee, yet another group of impartial industry experts, academics, and analysts who review the certification blueprint. This group reports significant developments in a subject area to CompTIA credential managers. If the committee recommends that additional technologies be addressed before a scheduled exam update, the development cycle is altered in order to cover all knowledge, skills, and abilities necessary to perform the job functions associated with cybersecurity—and yet another question-writing development cycle is added to the certification for that year.

As an example, since CompTIA Security+ was first published in 2002, CompTIA has provided regular updates and major revisions to this ANSI/ISO 17024-accredited certification.[5] SMEs from the government, academic, and private sectors meet regularly to ensure that the content of the examination remains relevant and accurate. As the technology has evolved and the threats and exploits have grown, so too has the response in providing timely and accurate training materials and best practices.

HOW IS A CERTIFICATION DELIVERED?

In conjunction with its authorized examination centers worldwide, CompTIA takes several precautions to mitigate unauthorized exam activity. Individuals who break the rules risk losing their credential and being reported to authorities and governing professional bodies. They also face legal prosecution if they divulge answers or other prohibited intellectual property relating to an examination.[6]

To deter cheating, a variety of proprietary technologies are employed. These include delivery and transmission of exams in encrypted formats, random scrambling of examination questions and answers, pools of thousands of potential questions to stem the brute-force memorization of answers, and digital forensics such as biometrics and time-per-question analysis. The objective is to ensure that a CompTIA security certification is ethically created and honestly earned. Further, CompTIA participates in forums with other credential providers to maintain the integrity and security of IT certification credentials.

5. Exams are updated with new questions every six to eight weeks. CompTIA has launched its third major revision of the exam.
6. Pearson VUE, Prometrics, and the Government Services Agency (GSA) through TestSmart are leading CompTIA testing partners. Incidentally, they are also the preferred testing providers for the DOD 8570 information assurance program.

What to Measure in A Credential Examination: Knowledge, Performance or Both?

There is an internal debate among cybersecurity practitioners as to what is more important to validate: 1) An individual's conceptual knowledge, or 2) Performance associated with a particular job or responsibility. Advocates for each of these two aspects of validation may hold one of the approaches as superior over the other. However, CompTIA regards this growing rift as a false dilemma. Both domain knowledge expertise and practical skills are absolutely vital and should be a part of any serious competency training and validation process.

When a certification is developed or updated, CompTIA works closely with its learning partners to ensure training materials are available in the industry and are available in multiple mediums. Both knowledge- and performance-based aspects are necessary for training, and nothing can substitute for hands-on learning. Moreover, a significant portion of testing for CompTIA certifications includes scenario-based questioning that asks the test taker to react to real-life situations.

A meaningful benefit in certifications that are predominately knowledge-based is that they help establish criteria or measure an individual's readiness and ability to move to higher-level and more complex certifications. This core base of knowledge provides confidence in situations not previously encountered and leads to the development of best practices, resulting from lessons learned in other settings. Psychometric validation that can accurately measure conceptual knowledge has existed for decades and is evident in the trustworthiness of high-stakes assessments such as the SAT, GRE, MDCAT, and LSAT.

We need to know how to drive the car, but we also need to know things about speed limits, right of way, and other conceptual knowledge before we can secure a driver's license. It's really not one or the other; it's a matter of authentically integrating both the practical and the foundational knowledge and then making sure that testing processes validate both types of knowledge. To ensure this, CompTIA has added performance- based questions to many of its certification exams and will continue to include them on all new and updated products.

Innovations that allow for test simulations will increasingly promote performance-based testing as appropriate for specific career paths and levels of expertise. In 2011, CompTIA introduced its first mastery-level certification exam in the cybersecurity domain, the CompTIA Advanced Security Practitioner (CASP) certification exam. This exam validates a higher level of skills required for both systems and network security. It is highly recommended that individuals taking this exam have a minimum of five years of technical security experience at the enterprise level. The CASP certification exam has a special software design that allows for simulation-based items.

As cybersecurity specializations develop, expertise will lean toward performance-based criteria but will also continue to be supported by a foundation of core conceptual knowledge—much like a surgical internship practically validates a medical student who has already passed his or her graduation requirements. The key is to make sure that such a process does not unnecessarily bottleneck the cybersecurity education and training ecosystem. We need cybersecurity professionals who are trained and credentialed in a timely manner.

The CompTIA Public-Private-Academic Partnership: Optimum Responsiveness to Rapid Developments in the Cybersecurity Threat Environment

The cybersecurity challenges of today — and tomorrow — are being confronted by dedicated professionals in the government, the private sector and academia working in a collaborative setting and utilizing the best available technical tools.

CompTIA certifications are an indispensable piece of an ecosystem that stands at the ready to protect this vital digital infrastructure. As an association, we have been engaged with various government agencies, academic partners and initiatives to ensure that industry-recognized certifications are a prominent piece of the overall national cybersecurity posture. Support for industry-recognized certifications is a fundamental tenant of the National Initiative for Cybersecurity Education (NICE).

As technology becomes more broadly used, cybersecurity awareness is important for the general workforce along with specialized security professionals. CompTIA research found that human error accounted for 55 percent of security breaches in 2013, and that number is growing every year. The NICE campaign has four components and it seeks to improve the cyber-behavior, skills and knowledge of the population-at-large in order to create a safer cyberspace. The components are:

- **National Cybersecurity Awareness.**
- **Formal Cybersecurity Education.**
- **Cybersecurity Workforce.**
- **Cybersecurity Workforce Training and Professional Development.**

As an early contributor to the NICE initiative, particularly as it relates to the professionalization and training of the nation's workforce, CompTIA provided input to NIST and the Department of Homeland Security (DHS) to help articulate standards for how the association defines cybersecurity roles and responsibilities. The goal of this component of the NICE process is that it will result in a common lexicon in terms of how various cybersecurity roles are defined and what knowledge, skills and abilities (KSAs) align to those roles across government. The resulting input from a broad cross-section of government, private sector and academic contributors (including CompTIA) was the establishment of 31 cybersecurity specialty areas that are now housed on a portal. The portal was designed to be an online resource for individuals looking to enter the cybersecurity workforce, advance their careers or simply want to be more cyber-savvy.[7]

CompTIA also engaged in a detailed mapping process to align its certifications to many of the cybersecurity specialty areas and jobs identified by DHS. In an effort to ensure a clear connection between CompTIA certifications and specialty areas, if the association's certifications did not address 85 percent of the KSAs within a specialty area, the exam was not presented as a viable test to validate skills for that specialty. CompTIA has also encouraged peer-credentialing bodies through our role as a founding member of the Cybersecurity Credentials Collaborative[8] to do the same.

7. http://niccs.us-cert.gov/
8. http://www.cybersecuritycc.org/

This mapping exercise will no doubt have important implications for academic and private sector settings. Additionally, NICE is working with the Office of Personnel Management (OPM) to ensure that this work has relevance and application to the federal workforce across all the agencies. A baseline definition of cybersecurity jobs will finally allow OPM to properly benchmark and identify gaps in the federal workforce. The objective is to support government professionals already employed and recruit new professionals who have identifiable skill-sets to ensure a sufficient and capable workforce is in place to protect the government's online environment.

Another piece to the puzzle is Executive Order 13636, entitled the "Framework for Improving Critical Infrastructure Cybersecurity." The Executive Order, which was issued in February 2013, established "it is the Policy of the United States to enhance the security and resilience of the nation's critical infrastructure and to maintain a cyber-environment that encourages efficiency, innovation and economic prosperity while promoting safety, security, business confidentiality, privacy and civil liberties."

The Executive Order charged NIST with developing a framework that is voluntary, risk-based and intended only for owners and operators of critical infrastructure. The framework is a set of industry standards and best practices designed to help organizations manage cyber risks. According to CompTIA research, only 41 percent of firms currently perform formal risk analysis as part of their security planning. For the purposes of the framework, critical infrastructure is defined as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

NIST worked closely with industry and government partners in the development of this framework organizing five workshops – three of which CompTIA participated in – and a call for public comment – to which CompTIA submitted recommendations.[9]

Through the Certified Academic Partnership Program (CAPP), CompTIA works with community colleges and other academic institutions. Many of these institutions are academic centers of excellence and serve as gateways for government recruiting in cybersecurity.

The partnership between government, academia and industry is a robust and strong one. By working with government partners, CompTIA is able to share resources and tools that have been created by the private sector for the development of a strong federal and private cyber workforce. These alliances with government and academia go far in ensuring a seamless workforce – one that can easily move from the public to the private sector, effectively share new knowledge and approaches, and always ensure that there is an adequate skilled labor force to ward off cybersecurity attacks and advance critical infrastructure needs.

> "For the last 10 years, what we've seen on our networks has been essentially exploitation, [such as] theft of intellectual property and crime. Over the last few weeks, we've seen distributed denial-of-service attacks, so we're seeing the threat grow from exploitation to … disruption, and my concern is it's going to go from exploitation and disruption to destruction."
>
> – Army Gen. Keith B. Alexander, Director of the National Security Agency
> Oct. 2, 2012

9. Refer to the NISTFramework pdf (http://techvoice.org/Libraries/Documents/CompTIA_Comments_NISTFramework_12-13-13.sflb.ashx)

CompTIA and the Cybersecurity Credentials Industry

As domain areas in cybersecurity continue to evolve, there is a corresponding increase in credentials that validate new skill sets. While proliferation of credentials can lead to confusion, in most cases the distinctions among them can be understood when one considers the particular domain addressed, as well as the complexity of the skill and any reference to vendor-specific or vendor-neutral expertise.

A simple but important way to distinguish valid credentials from "fly-by-night" entrants is to consult the ANSI.[10] ANSI maintains a personnel certification accreditation program, and governmental agencies in key sectors such as national security, public safety, and healthcare rely on ANSI accreditation for third-party verification of the competence of certification bodies. ANSI is the only personnel certification accreditation body in the U.S. to fulfill the globally recognized requirements of ISO/IEC 17011:2004, which represents the highest internationally accepted practices for accreditation bodies.

CompTIA also works closely and collaboratively through meetings and engagements with peer certification organizations and stakeholders in government, academia, and the private sector. The shared objective is to align credentials to identified career pathways, inform senior IT leadership and the educational community about the role of cybersecurity credentials, and provide continuous improvement and management of the credentialing ecosystem. It is incumbent upon those in the IT security credentials world to align various organizations and vendor companies to publicize more coherent and interrelated career paths—from entry-level to mastery levels of IT expertise. IT professionals will continue to inspire trust and support from IT and HR personnel in the cybersecurity world.

GLOSSARY

ANSI American National Standards Institute, a 501(c)(3) non-profit association and the voice of the U.S. standards and conformity assessment system. While helping to assure the safety and health of consumers and the protection of the environment, ANSI oversees the creation, promulgation, and use of thousands of norms and guidelines that directly impact businesses in nearly every sector—from acoustical devices to construction equipment, from dairy and livestock production to energy distribution, and many more. ANSI is also actively engaged in accrediting programs that assess conformance to standards, including globally recognized cross-sector programs such as the ISO 9000 (quality) and ISO 14000 (environmental) management systems.

Bloom's Taxonomy A classification scheme of intellectual behavior developed by Benjamin Bloom who identified six levels of cognitive learning—from the simple recall of facts (Knowledge), as the lowest level, through the increasingly complex levels of Understanding, Application, Analysis, Synthesis, and Evaluation.

CompTIA A+ Certification The CompTIA A+ certification is the industry standard for

10. Refer to the ANSI Accreditation Directory (https://www.ansica.org/wwwversion2/outside/PERdirectory.asp?menuID=2)

computer support technicians. The international, vendor-neutral certification proves competence in areas such as installation, preventative maintenance, networking, security, and troubleshooting. CompTIA A+ certified technicians also have excellent customer service and communication skills to work with clients.

CompTIA Advanced Security Practitioner (CASP) CASP is CompTIA's first mastery level certification exam and was voted on to the DoD 8570 exam list in early 2013. CASP is approved for IAT Level III, IAM Level II, IASAE Level I, and IASAE Level II in U.S. DoD Information Assurance directive 8570.01-M. It is designed for information assurance professionals in technical leadership roles in an IT enterprise environment (especially military environments). CASP proves competence in enterprise security; risk management and incident response; research and analysis; integration of computing; communications and business disciplines; and technical integration of enterprise components.

CompTIA Network+ Certification The CompTIA Network+ certification is the sign of a competent networking professional. It is an international, vendor-neutral certification that proves a technician's competency in managing, maintaining, troubleshooting, installing and configuring basic network infrastructure. Since its introduction in 1999, more than 235,000 people have become CompTIA Network+ certified.

CompTIA Security+ Certification CompTIA Security+ is an international, vendor-neutral certification that proves competency in system security, network infrastructure, access control, and organizational security.

Critical IT Infrastructure The backbone of our nation's economy, security and health. We know it as the power we use in our homes, the water we drink, the transportation that moves us, and the communication systems we rely on to stay in touch with friends and family. Critical infrastructure are the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. (http://www.dhs.gov/what-critical-infrastructure)

Cyberspace Cyberspace is a global domain within the information environment consisting of the interdependent network of IT infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

Cybersecurity A synonym of Information Security as cited in ISO 27001.

Examination Blueprint is a document related to a particular area of domain knowledge, composed of one or many learning objectives. A learning objective answers the question: What is it that an individual should be able to do or know? A learning objective makes clear the intended learning outcome rather than what form the instruction will take. Learning objectives focus on student performance. Action verbs that are specific, such as list, describe, report, compare, demonstrate, and analyze should state the behaviors students are expected to perform. Clearly defined objectives form the foundation for selecting appropriate content, learning activities, and assessment measures. (From Patricia Archer, 1979, Writing Higher-Level Learning Objectives: The Cognitive Domain, New York: Media Systems Corporation)

Global Information Grid The globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to war fighters, policy makers, and support personnel. The global information grid includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and national security systems. Also called GIG.

Global Information Infrastructure The worldwide interconnection of communications networks, computers, databases, and consumer electronics that make information available to users. The global information infrastructure encompasses a wide range of equipment, including cameras, scanners, keyboards, facsimile machines, computers, switches, compact disks, video and audio tape, cable, wire, satellites, fiber optic transmission lines, networks of all types, televisions, monitors, printers, and much more. The friendly and adversary personnel who make decisions and handle the transmitted information constitute a critical component of the global information infrastructure. Also called GII.

Information Assurance Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (DOD 8500.01E, October 24, 2002, recertified April 23, 2007)

Information Security is defined as the preservation of the confidentiality, integrity, and availability of information. Additionally, other properties such as authenticity, accountability, non-repudiation, and reliability can also be involved (ISO/IEC 17799:2005). Also see NIST 800-30, "Information system security is a system characteristic and a set of mechanisms that span the system both logically and physically. The five security goals are integrity, availability, confidentiality, accountability, and assurance."

ISO The Independent, non-governmental membership organization and the world's largest developer of voluntary International Standards. (http://www.iso.org/iso/home/about.htm)

Job Task Analysis (JTA) The formal process of defining the requirements of a position and identifying the knowledge, skills, and abilities necessary to effectively perform the duties of the position. (www.hss.energy. gov/DepPersonnelSec/hrp/html/glossary.htm)

Malware Software such as viruses or "Trojan Horse" programs designed to cause damage or disruption to a computer system.

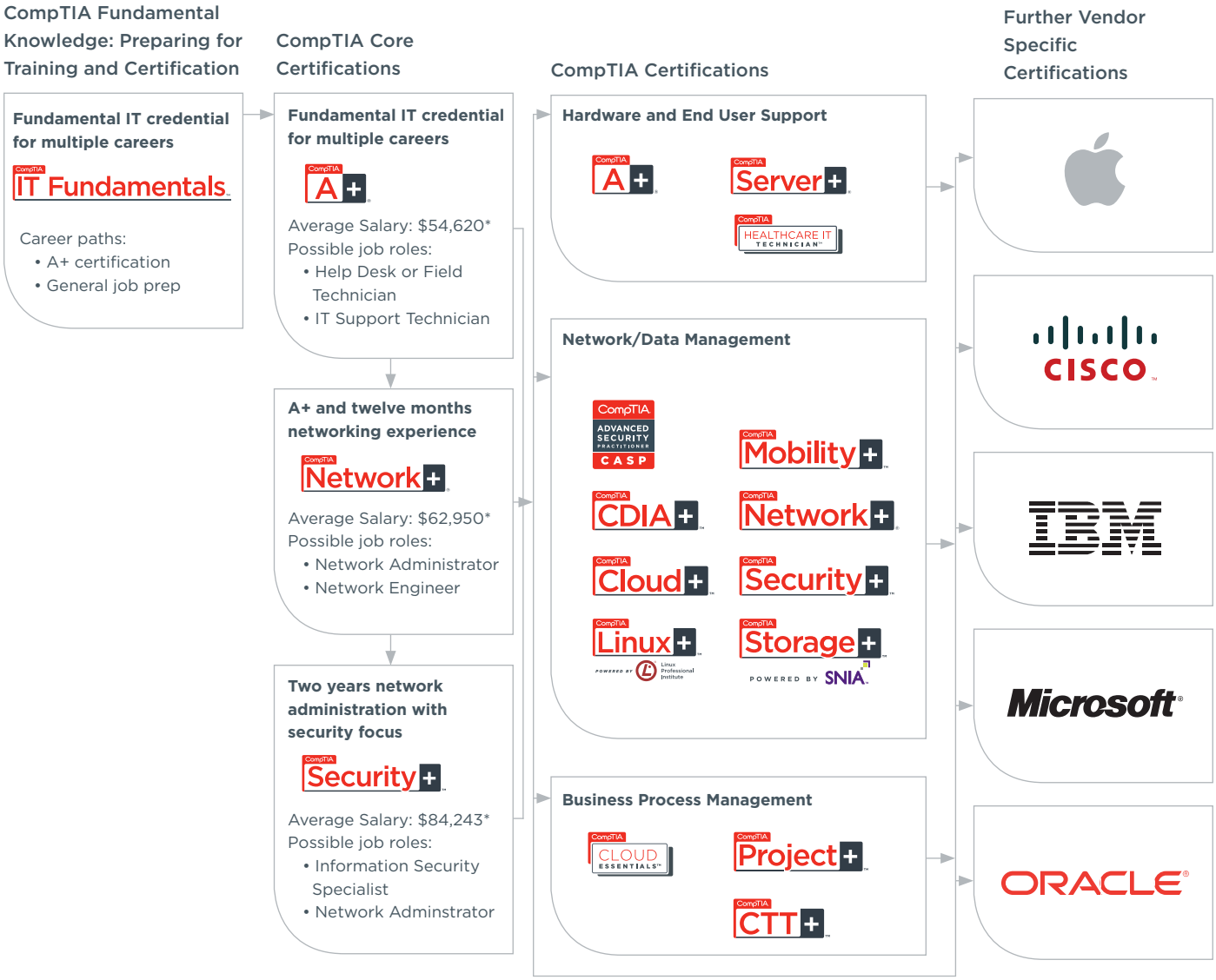
Psychometrics Psychometrics is the field of study concerned with the theory and technique of educational and psychological measurement, which includes the measurement of knowledge, abilities, attitudes, and personality traits. The field is primarily concerned with the construction and validation of measurement instruments, such as questionnaires, tests, and personality assessments. It involves two major research tasks, namely: (i) the construction of instruments and procedures for measurement; and (ii) the development and refinement of theoretical approaches to measurement. Those who

practice psychometrics are known as psychometricians and although they may also be clinical psychologists, they are not obliged to be so and could instead be, for example, human resources or learning and development professionals. Either way specific, separate qualifications in psychometrics are required.

Subject Matter Expert (SME) An SME or domain expert is a person who is an expert in a particular area or topic. When spoken, sometimes the acronym «SME» is spelled out («S-M-E») and

Appendix 1

CAREER ROADMAP



* Source: Computerworld Salary Survey 2013 - U.S. salaries only

Appendix 2

CERTIFICATION EXAM DEVELOPMENT PROCESS

Job Task Analysis & Blueprint Development

- Need Arises for the Development of a Certification Examination
- Selection of Subject Matter Experts (SMEs)
- Job Task Analysis (JTA) Workshop, CompTIA HQ
- Output: Preliminary JTA and Preliminary Examination Objectives Blueprint (EOB)

Preliminary JTA and Exam Objectives: Blueprint Validation

- Statistical survey to validate Preliminary Blueprint (Statistically significant number of respondents needed; global feedback opportunity)
- Output: Working Examination Objectives Blueprint released globally (translated)
- Curriculum & training development initiated with 3rd-party providers

Preliminary Exam Development & Validation

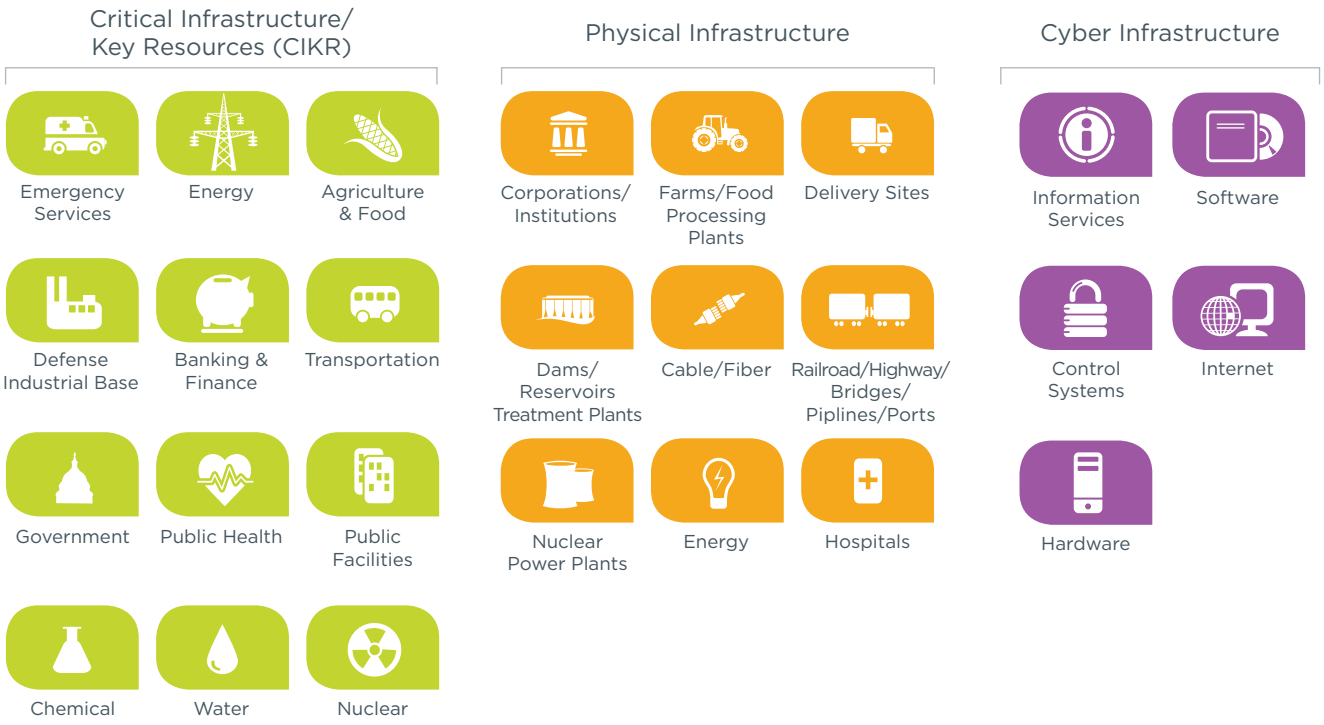
- Exam Item-writing workshop (12-15 SME participants, CompTIA HQ
- Output: Beta Examination to be published globally by CompTIA test providers
- Beta Examination taken and validated by statistically significant beta test population & feedback
- Output: Final Certification Examination

Exam Publication and Release

- Examination localization & translation(s) development
- Examination release (timed to coincide with availability of 3rd-party curricular materials)
- Annual updates to create additional items for the examination question pool
- Regular refresh of all content to assure accuracy and currency of domain knowledge validated

Appendix 3

CYBERSPACE INFRASTRUCTURE RELATIONSHIPS[11]



11. Adapted from "Securing the Nation's Critical Cyber Infrastructure," US Department of Homeland Security

About CompTIA

CompTIA is the voice of the world's information technology (IT) industry. Its members are the companies at the forefront of innovation and the professionals responsible for maximizing the benefits organizations receive from their investments in technology. CompTIA is dedicated to advancing industry growth through its educational programs, market research, networking events, professional certifications, and public policy advocacy.

For more information, please visit CompTIA.org.

CompTIA Worldwide Headquarters
CompTIA Member Services, LLC
3500 Lacey Road, Suite 100
Downers Grove, Illinois 60515

630.678.8300

CompTIA.org