CCSP®

Cloud Security Skills Can Take Your Career to Infinity (And Beyond)

The Cloud Security Landscape

Cloud computing is omnipresent. Companies are rapidly migrating workloads from their on-premises data centers to the cloud, utilizing new technologies such as serverless, containers and machine learning to reap the benefits the cloud is delivering: flexible capacity and scalability, improved availability, and increased agility.

With constant access to content, apps and devices – all seamlessly connected to each other, without disruption – cloud computing is an inextricable part of our everyday lives. A recent report by Thales[1] indicates that 98% of global organizations store some kind of sensitive data in the cloud. 95% use Software-as-a-Service (SaaS) applications, 67% Infrastructure-as-a-Service (IaaS) platforms and 65% Platform-as-a-Service (PaaS) environments.

Despite the many advantages that come with adoption of cloud computing, organizations are faced with new challenges and concerns. Among them, security remains a key issue.[2] In fact, 94% of cybersecurity professionals confirm they are at least moderately concerned about cloud security.

With more cyberattacks targeting cloud workloads, organizations need to become more confident about their cloud security posture. Organizations in all industries and sectors are hiring cloud security accredited professionals to address the challenges of the expanding threat landscape. But adoption of effective cloud security does not come without barriers. The 2020 Cloud Security Report revealed that the biggest challenges organizations face are not related to technology, but to people and processes. The survey indicated staff expertise and training (55%) is the biggest barrier, followed by budget challenges (46%), data privacy concerns (37%), and lack of integration with on-premises platforms (36%).

According to the 2020 Cybersecurity Workforce Study, despite the workforce shortage decreasing this year, employment in the field still needs to grow by approximately 41% in the U.S. and 89% worldwide in order to fill the talent gap in cybersecurity, and cloud computing security is by far the most in-demand skill set[3].

Rethinking Security in Cloud Environments

Cloud is convenient, but it can also become a vulnerability. The cloud security skills gap means companies are scrambling to fill cloud security positions. In fact, recent surveys indicate that organizations are seeking to train and

certify IT staff interested in transitioning to cybersecurity to assure their evolving security needs are met. As a result, 40% of industry professionals plan to pursue cloud security training within the next two years. This rate will continue to grow as organizations turn to cloud-based solutions versus on-premises legacy ones[4].

Professionals need to rethink security, as cloud services, platforms and environments are adopted by more and more by organizations. In 2020, nearly a third of organizations have identified a challenge in locating individuals capable of managing converged infrastructures that blend traditional and cloud systems into a coherent networked environment. Security professionals must ensure a holistic and effective approach to cloud security.

To successfully protect the organization, practitioners must reconsider security to include key components in the cloud:

- Data
- Users
- Applications
- Connectivity
- Infrastructure

Cloud security professionals should govern and protect all cloud components to avoid security gaps, keeping users and data safe. To achieve that, practitioners need to:

- Secure access to web content and cloud apps for any user, anywhere, and on any device
- Have visibility and control across the organization to drive cloud security strategy
- Safeguard data as it moves to and from the cloud
- Enable direct-to-cloud connectivity for users and sites without backhauling
- Optimize infrastructure and workflow
- Protect against advanced threats, including zero-day exploits

A common trap practitioners fall for is using traditional security practices and tools to safeguard cloud workloads. Unfortunately, most legacy security tools are not designed for the dynamic, distributed, virtual environments of the cloud. 82% of 2020 Cloud Security survey[5] respondents say traditional security solutions either do not work at all in cloud environments or have only limited functionality.

Lack of adequate security protections creates holes which bad actors are eager to exploit. According to the 2020 Cloud Security Report, the biggest security threats are misconfiguration of the cloud platform (68%), unauthorized access (58%), insecure interfaces (52%), and hijacking of accounts (50%). The Thales Data Threat 2020 report[6] indicates that 49% of global respondents experienced a breach affecting data in the cloud.

Organizations are increasingly investing in either hiring or training security professionals to address these vulnerabilities. With such a high demand for cloud security professionals, demonstrating a sound understanding of cloud security principles and practices opens a wide variety of prospects and promises a bright future.

Cloud Security Skillset

Protecting an organization's assets in the cloud from configuration errors and external threats is not an easy feat. Cybersecurity professionals must know how to plan and implement security strategies to reduce risk and

enhance protection; understand legal and ethical issues associated with information security, privacy, and digital rights; and have core knowledge surrounding cloud computing and security best practices.

A solid foundation of technical skills and contextual understanding of threats in the cloud are particularly necessary because attacks cybersecurity professionals encounter today are the result of adversaries exploiting yesterday's poorly designed systems and vulnerabilities. Someone with a strong foundation will be able to understand the potential of emerging attacks in cloud and guide security teams to mitigation. Without this foundational knowledge in cloud security, the practitioner might be able to survive on a daily basis, but there's no guarantee that they will be able to respond to a security incident.

Because cybersecurity is such an in-demand field, professionals choosing this career path have a bright future. According to the Bureau of Labor Statistics[7], the cybersecurity industry is expected to grow by 31% until 2029, compared with the 4% growth rate across all industries. Moreover, according to some estimates[8], the global cybersecurity workforce will have more than 3.5 million unfilled positions by 2021.

As organizations continue to value security, and as adversaries continue to challenge the integrity and confidentiality of data in the cloud systems and the security measures in place to protect them, the cybersecurity industry will continue to need skilled professionals. A solid understanding of cloud security is a great asset for any individual, because they can differentiate from their peers and develop more career opportunities.

The Shared Responsibility Model

The need for skills and foundational knowledge of cloud security is underpinned by the fact that cloud security functions are a shared responsibility between the cloud providers and the organization using them. Whether you are using IaaS, PaaS, SaaS or a mix of platforms, major cloud vendors such as AWS[9], Azure[10] and Google Cloud[11] dictate that cloud security follows a shared responsibility model:

- Cloud providers are responsible for the security ***of*** the cloud.
- Cloud customers are responsible for the security ***in*** the cloud.

Cloud providers are responsible for protecting the infrastructure that runs the services they offer. This infrastructure comprises the hardware, software, networking and facilities that run cloud services. On the other hand, cloud customers assume full responsibility for the data they store on cloud platforms, their applications and operating systems, updates, and security patches, as well as the network and firewall configuration. In addition, customers are responsible for the identity and access management controls they implement to authenticate and authorize access to the data, and for the encryption of the data at rest and in transit.

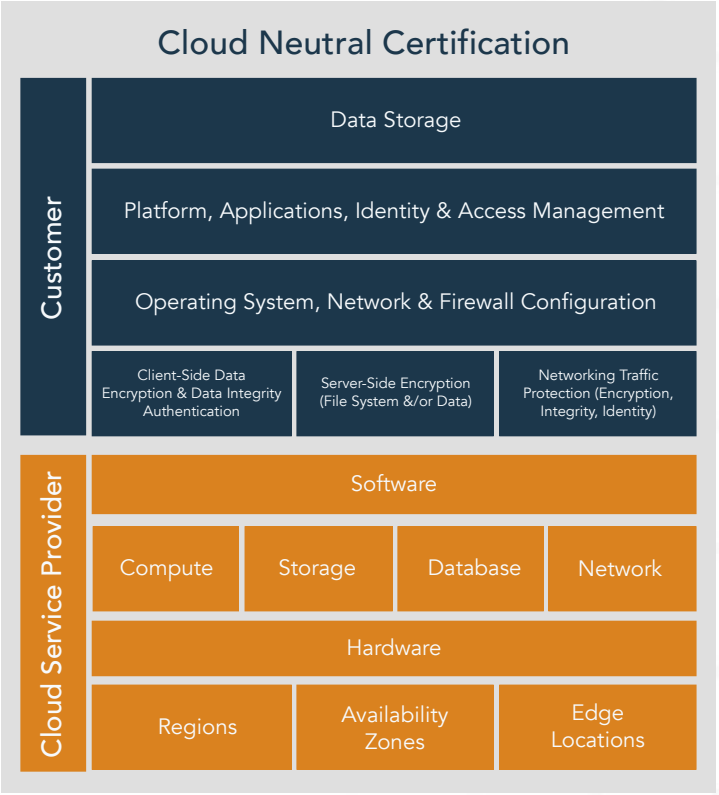


Figure 1: The Shared Responsibility Model.

The shared responsibility model is the foundation of cloud security. Cloud security professionals need to have a solid understanding of their roles and responsibilities. Having a false understanding of their level of responsibilities in the cloud can lead to misconfigurations and poor

security controls. Cloud workloads are entry points to the organizations' networks and bad actors are eager to exploit any gaps in the cloud security posture.

Technical Skills

Security professionals need to have the right mix of technical and soft skills to thrive in cloud security. While the technical skill set proves you have the foundational knowledge to apply best practices for securing cloud environments, the soft skills enable cloud security professionals to emerge as true leaders no matter their position in an organization's hierarchy.

Technical skills cover a wide breadth of knowledge. To begin with, the cloud security professional should understand the cloud computing building blocks, such as definitions, roles and technologies. In addition, they should possess a foundational knowledge of the relevant security and design principles for cloud environments, such as cryptography, access control, virtualization security and vendor lock-in.

Furthermore, they need to have the knowledge to implement data discovery and classification technologies relevant to cloud platforms and to design and apply data protections for personal and sensitive data in the cloud to meet regulatory compliance requirements, such as GDPR, HIPAA and CCPA. The cloud security professional will have to identify and classify critical information and plan and execute datacentric measures to eliminate or reduce the potential of adversary exploitation.

In addition to protecting the data in the cloud, security professionals need to have knowledge of the risks and threats to the cloud infrastructure components – both physical and virtual – and the controls to mitigate these threats.

As organizations depend on cloud applications to deliver services, security professionals will also need to focus on ensuring the security of these apps, understand the concepts of software assurance and validation, and verify the security of the software using applicable controls.

Finally, the cloud security professional should be aware of the various ethical and legal constraints and techniques to be able to determine a criminal act and safeguard the integrity and confidentiality of the data in the cloud.

These cloud-specific technical skills can assist cloud security professionals in meeting both business and security requirements in any industry vertical or regulatory framework.

Soft skills

Besides technical skills, soft skills are also important for the professional who wishes to excel in the field of cloud security. The ability to solve complex problems

is critical and helps to analyze issues properly, clearly convey technical issues with colleagues, and drive quick conclusions. Making effective business and security decisions is also a core value for all professionals in modern business environments.

Security professionals need strategic thinking to lead business operations, observe trends, balance between long- and short-term objectives, and set priorities. In addition, they need to be able to communicate effectively and advocate cloud security principles and best practices. With an abundance of available solutions and technologies, being able to select and implement fit-for-purpose technologies and reap all their benefits is equally important.

In a constantly changing global and business environment, professionals must be flexible to adapt to the changes, and they need to have a holistic view of the environment, abstracting from technical details and viewing operational business objectives as an entity.

Cloud Security Knowledge to Boost Your Career

To gain the specific skill set required for building a solid foundation as a cloud security professional, industry training and certification create a proven path to success. Cloud security training specifically focuses on the operational knowledge you need to configure the platform and avoid costly mistakes. Certification broadens the knowledge and provides you with the big picture about cloud computing and security.

A cloud security certification will help you understand concepts like legal compliance, roles and responsibilities, and alignment of security objectives with the organization's goals. The knowledge acquired through a certification process coupled with your background and experience can boost your career to new heights.

Benefits to Your Career at Any Stage

The knowledge and skills earned by holding a cloud security certification are important at any stage of your career. Whether you are at an early development stage, transitioning from IT, changing your career path or a senior executive, there is a lot to learn about this fast-evolving technology.

Cloud security is such an integral part of business operations, the structured and disciplined knowledge earned while pursuing a cloud security certification can only enhance your prospects among the thought leaders in your organization.

Establishing a Career Path

As you build your career, cloud security certification will help you become a valuable asset to your team and manager. The right credential enables you to translate and implement effective cloud security policies into well-established, robust practices and solutions to protect the organization's data from the prying eyes of cybercriminals.

Building Your Career as Cloud Security Specialist

On the other hand, if you have already worked to establish a career as a prominent and proficient IT or security practitioner, the cloud security certification will arm you with the unique cloud-specific knowledge and skill set professionals are increasingly required to have. This disciplined knowledge will assist you to align business objectives with security solutions and be an enabler of increased productivity and success.

Achieving Mastery of the Cloud

As a security expert, the foundational knowledge gained from a cloud security certification can help you develop strategies to drive your organization forward to innovation and success. Understanding how secure cloud computing can propel your organization to increase business revenue will assist you to make the right decisions and align you to be a leader in your company now and in the future.

With cloud security job openings at a record high and growing, there has never been a more advantageous time to earn your cloud security certification. With countless benefits presented by pursuing a cloud security certification, the challenge now is to select the one which will satisfy all your needs.

Command the Cloud with CCSP

The (ISC)² Certified Cloud Security Professional (CCSP) is the credential that can take your career to the clouds and beyond. CCSP is the benchmark of cloud security certifications and is repeatedly recognized as the most valued and well-rounded cloud security certification available[12].

Pursuing CCSP certification benefits practitioners and gives them the competitive advantage in an increasingly competitive landscape. The CCSP is authoritative and exemplifies the commanding leadership essential for ensuring that cloud security is holistically incorporated into every cloud solution, utilizing a vast knowledge base and a disciplined skill set.

A Vendor-Neutral Certification

CCSP is a vendor-agnostic certification, ensuring certified practitioners have the security knowledge to successfully secure any cloud environment.

With more organizations opting for vendor-neutral cloud security solutions to avoid vendor lock-in, the neutrality of CCSP certification is a great bonus for cloud security practitioners seeking to apply effective controls, policies and configuration best practices over a variety of platforms. The biggest advantage of a vendor-neutral certification is it gives the practitioner a balanced approach and knowledge base of all aspects of cloud computing security, including the advantages and limitations of these technologies. Vendor certifications provide training only for their own platforms, which limits the scope and applicability of the knowledge gained.

Even if you already hold a vendor-specific certification, you can still pursue the CCSP credential to build the end-to-end foundational knowledge needed for effective cloud security. CCSP can extend your skills and allow you to apply your security expertise to multiple cloud computing environments, demonstrating competence in cloud architecture, design, operations, data security, risk and compliance. The vendor-neutral knowledge gained by achieving CCSP certification ensures your ability to protect sensitive data in any cloud environment.

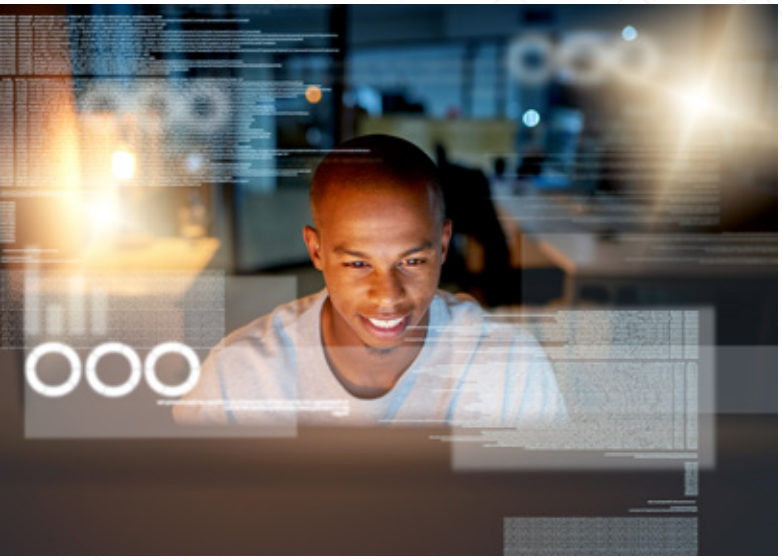
A Market Differentiator

The CCSPs unique criteria have elevated it to a standard that has allowed it to be identified as the premier cloud security certification. With numerous reasons identified as its differentiator, giving it an unsurmountable advantage when compared to other certifications, it also presents its certification holders benefits that give them the competitive advantage in an increasingly competitive landscape.

Competent Knowledge. A CCSP is positioned as a subject matter expert on cloud security, proving proficiency to keep up with new technologies, developments and threats.

Solid Foundation. The CCSP certification provides the advanced knowledge and skills required to establish cloud security best practices, evolving technologies and mitigation strategies.

Career Progression Opportunities. The CCSP certification opens a variety of job opportunities since almost all organizations now operate to some degree in the cloud and robust cloud security posture is a key factor to allow them to innovate and gain competitive advantage.



Industry Recognition. Cloud security practitioners expand their knowledge on cloud services and their security through continuous professional development with CPE activities, gaining recognition from organizations who seek to move securely to the cloud and innovate.

Increased Compensation. The CCSP certification can help increase your earnings. Professionals with a CCSP certification are ranked #5 on the Certification Salary Survey list[13].

Professional Credibility. The CCSP certification helps enhance professional credibility by demonstrating commitment and dedication to the cybersecurity profession. The certified professional conveys knowledge and inspires trust, improving their future marketability into leadership positions.

Peer Networking. Acquiring the CCSP certification enhances networking opportunities with other certified and skilled cloud security professionals who can become an invaluable repository of knowledge and information when the need arises.

Blend New Knowledge with Business Goals. The knowledge gained by attesting the CCSP exam helps professionals understand all areas of cloud deployment and how cloud services and security relate to business objectives, risk tolerance and regulatory compliance. The alignment of cloud technology and security with business strategic goals is a market differentiator and a great return on the certification investment.

Proof of Understanding the Cloud Environment. The CCSP certification is proof of understanding the technology behind cloud platforms which can help you make better decisions for budgeting, staffing, organizational structure and outsourcing.

Improved Work Performance. Understanding emerging cloud technology and security principles can help you improve your work performance by leveraging all the benefits cloud environments offer for enhanced collaboration.

Mentor the New Generation. Tenured pros can mentor the next generation of IT security professionals based on knowledge and experience of security collaboration and integration. Passing on wisdom helps create a security culture that fosters a robust cloud security posture.

Earning the CCSP proves you are at the forefront of cloud security. We asked CCSP-certified cybersecurity professionals how they benefited from earning this certification, and they said:

"One of the greatest benefits of completing the CCSP was industry recognition by employers. With a more significant number of organizations undergoing modernization and cloud migration efforts, there is a strong demand for cyber professionals to secure these environments. The CCSP prepared me to understand security concerns surrounding various cloud deployment and service models, which enabled me to create a roadmap to overcome common challenges during security control implementation. Organizations moving to cloud environments or consuming cloud services must be aware of potential security risks. As a CCSP, I'm confident in my ability to be the security advocate and trusted advisor for securing cloud deployments."
—Hunter Sekara, CISSP-ISSAP, ISSEP, ISSMP, SSCP, CCSP, CAP, CSSLP

"Achieving CCSP helped enhanced my professional credibility. It helped demonstrate my commitment and dedication to the profession and brings significant value to my career including promotion opportunities."
—Babatunde Falode, CISSP, CCSP

"It enables me to catch up with the new generation of young IT professionals who haven't made the journey from the mainframe to the cloud."
—Paul Oor, CISSP, CCSP

How CCSP Stands Out

The certification stands out among other cloud security certifications for many excellent reasons. Certification Magazine calls the CCSP "the most well-rounded certification by far for the cloud protection area[14]" and has ranked it as the #1 certification their survey respondents plan to earn. CCSP is the only cloud security credential that requires cloud experience. Candidates must have a minimum of 5 years' experience in IT, of which 3 years must be in information security and 1 year in cloud security.

The versatility and neutrality of CCSP knowledge has made it a credible qualification toward internationally recognized cloud standards, such as ISO/IEC 17024, 17788, 17789, 27017 and 27018. Through a continuous professional education and development scheme, CCSP-certified professionals stay current on emerging threats, technologies, regulations, standards and practices, ensuring their ability to protect sensitive data in a global environment.

CCSP Gives Your Career the Competitive Advantage

The CCSP is an essential partner for you to excel in cloud security at any stage of your career. With the cloud security skill set earned, you will be able to better manage the power of cloud computing while keeping critical assets in secure. With CCSP, the sky is your limit.

The CCSP shows you have the advanced technical skills and knowledge to design, manage and secure data, applications and infrastructure in the cloud using best practices, policies and procedures established by (ISC)².

The structured knowledge earned by holding the CCSP certification is a sure path to your career success and your organization gaining competitive advantage in a shifting global environment. The CCSP certification can take your career to infinity and beyond.

To learn more about how the CCSP credential can help you gain expertise and advance your career, visit https://www.isc2.org/Certifications/CCSP, and download our 20 Tips for Secure Cloud Migration eBook.

About (ISC)²

(ISC)² is an international nonprofit membership association focused on inspiring a safe and secure cyber world. Best known for the acclaimed Certified Information Systems Security Professional (CISSP®) certification, (ISC)² offers a portfolio of credentials that are part of a holistic, programmatic approach to security. Our membership, more than 150,000 strong, is made up of certified cyber, information, software and infrastructure security professionals who are making a difference and helping to advance the industry. Our vision is supported by our commitment to educate and reach the public through our charitable foundation – The Center for Cyber Safety and Education™. For more information about (ISC)² visit our website, follow us on Twitter or connect with us on Facebook.

References

1 Thales Data Threat 2020 Report, Global Edition, available at https://cpl.thalesgroup.com/data-threat-report

2 Cybersecurity Insiders 2020 Cloud Security Report, available at https://www.cybersecurity-insiders.com/portfolio/2020-cloud-secuity-report-isc2/

3 (ISC)² 2020 Cybersecurity Workforce Study https://www.isc2.org/Research/Workforce-Study

4 (ISC)² 2020 Cybersecurity Workforce Study https://www.isc2.org/Research/Workforce-Study

5 Cybersecurity Insiders 2020 Cloud Security Report, available at https://www.cybersecurity-insiders.com/portfolio/2020-cloud-secuity-report-isc2/

6 Thales Data Threat 2020 Report, Global Edition, available at https://cpl.thalesgroup.com/data-threat-report

7 Bureau of Labor Statistics, Occupational Outlook Handbook, Information Security Analysts, available at https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

8 Cybercrime Magazine, Cybersecurity Talent Crunch To Create 3.5 Million Unfilled Jobs Globally By 2021, available at https://cybersecurityventures.com/jobs/

9 Amazon Web Services, Shared Responsibility Model, available at https://aws.amazon.com/compliance/shared-responsibility-model/

10 Microsoft, Shared responsibility in the cloud, available at https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

11 Google Cloud Platform: Shared Responsibility Matrix, available at https://services.google.com/fh/files/misc/gcp_pci_srm__apr_2019.pdf

12 Cybersecurity Insiders 2020 Cloud Security Report, available at https://www.cybersecurity-insiders.com/portfolio/2020-cloud-secuity-report-isc2/

13 Certification Magazine, Salary Survey 2019: Certification leads to improved performance, increased earning power, available at http://certmag.com/salary-survey-2019-certification-leads-improved-performance-increased-earning-power/

14 Certification Magazine, Salary Survey 2019: Certification leads to improved performance, increased earning power, available at http://certmag.com/salary-survey-2019-certification-leads-improved-performance-increased-earning-power/