CCSP®

Certified Cloud Security Professional

An (ISC)² Certification

20 TIPS FOR SECURE CLOUD MIGRATION

Advice & Insights from Certified Cloud Security Professionals

As organizations increasingly make the transition to the cloud, cybersecurity practices are shifting to a cloud-based paradigm.

According to the latest Thales Data Threat report, **98% of surveyed organizations have some sort of sensitive data in the cloud**. In addition, these organizations are increasingly relying on multiple cloud platforms to reap the benefits of scalability, flexibility, availability and reduced costs. However, cloud environments are not without security challenges and vulnerabilities.

Cloud security is a key concern for organizations. The main challenge organizations migrating to the cloud face is creating a consistent security posture across their on-premises and cloud-based resources. The reality is that traditional security policies are not adequate to effectively and seamlessly implement robust security across a cloud environment. Organizations, therefore, need to turn to dedicated cloud-based security solutions to address cloud-related risks and challenges.

Cloud security is also a key concern for cybersecurity professionals as they work to broaden their cloud skills to meet these challenges.

Qualified cloud security professionals are **an essential factor for securely migrating to the cloud**. They provide valuable expertise and knowledge to all stakeholders throughout the migration process – from the initial planning stages to the deployment and everyday operations to ensure that their organization can enhance collaboration and innovation in the cloud.

To help organizations navigate in safe waters, we have asked Certified Cloud Security Professionals to offer advice and insights on the steps an organization should consider when planning to migrate to the cloud securely.

CCSP®

Certified Cloud Security Professional

An (ISC)² Certification

Contents

Section 1: Assess Your Current Infrastructure and Readiness

1. In-depth analysis of requirements
2. Rationalize assets
3. Classify and understand
4. Modernize

Section 2: Establish a Plan

5. Security from the outset
6. Security in every component
7. Understand dependencies
8. Take a phased approach

Section 3: Consider the Security Risks

9. Understand the attack surface
10. Cloud is a unique environment
11. Risk & responsibility remains
12. Need for strong encryption

Section 4: Prepare and Maintain Compliance

13. Responsibility does not get outsourced
14. Get guidance from auditors
15. Relevant legislation at storage locations
16. Assess the need for new co ntrols

Section 5: Prepare Your Team

17. Assess roles and responsibilities
18. Dedicated cloud team
19. Ensure robust knowledge and skills
20. Provide training

CCSP
Certified Cloud Security Professional
An (ISC)² Certification

Assess Your Current Infrastructure & Readiness

Once organizations have defined their business objectives and the strategy to materialize these objectives by migrating to the cloud, they need to review their infrastructure and assess the feasibility. A certified security professional can become a great asset in this step as the foundational knowledge on cloud security can blend with business objectives to facilitate an in-depth review of the current status.

- Start with In-depth Analysis
- Rationalize the Assets
- Classify and Understand Your Data
- Evolve Your Security

CCSP® Certified Cloud Security Professional

An (ISC)² Certification

Start with In-depth Analysis

Obtaining visibility into your organization's infrastructure, data and applications is the foundation of every security policy. You need to have a deep understanding of the application dependencies and perform a cost-based analysis to determine the real cost of upgrading to the cloud versus the expected added value.

> *There are no shortcuts: Always start with an in-depth analysis of the application requirements, dependencies and the relations with the underlying infrastructure.*

Carlos Lopez,
CISSP, CCSP,
Security Correlation Engineer,
San Jose, Costa Rica

CCSP Certified Cloud Security Professional
An (ISC)² Certification

Rationalize the Assets

Organizations depend on applications to deliver services and products to their customers. Review and assess the feasibility of moving these applications to the cloud as some apps may be cloud-ready, while others will have to be modernized. Depending on the results of the analysis, you may need to opt-in for a hybrid deployment model, where some of your applications and data will continue to reside on-premises, while others will migrate to the cloud.

Certified Cloud Security Professional
CCSP®
An (ISC)² Certification

> *Application Rationalisation: Understand your applications landscape and identify if applications can be ported to the cloud. Some applications can be lifted and shifted to cloud, but some require development to be cloud native.*

Jana Subramanian,
CISSP, CCSP,
Principal Cybersecurity Advisor,
Singapore

Classify and Understand Your Data

Data identification and classification is the first step to effective data protection. It is essential to identify what and where your data is and assess their criticality and sensitivity. Once you have classified your data, you can then select the appropriate controls to safeguard them. Corporate and personal data are lucrative targets for bad actors who always try to find gaps in data protection to steal or compromise data, then use it to launch other attacks against corporate networks such as impersonation or business email compromise.

Certified Cloud Security Professional

CCSP®

An (ISC)² Certification

“Classify and understand your data. Follow its lifecycle and protect it with appropriate security controls. Data has a very different risk profile once it is out of your ‘house’ or controlled. Do not take that lightly.”

Shan Shan Au Yeung,
CISSP, CCSP,
Group Information Security Manager,
Singapore

Evolve Your Security

Your security will have to evolve together with your infrastructure. Traditional, perimeter-based security controls are not adequate in a native cloud, multi-cloud or hybrid environment. Assess your security policies and practices to understand which can be used to secure your data and applications in the cloud. Your security posture will need to afford the same effectiveness in the cloud as on-premises and address cloud risks and challenges.

Certified Cloud Security Professional

CCSP®

An (ISC)² Certification

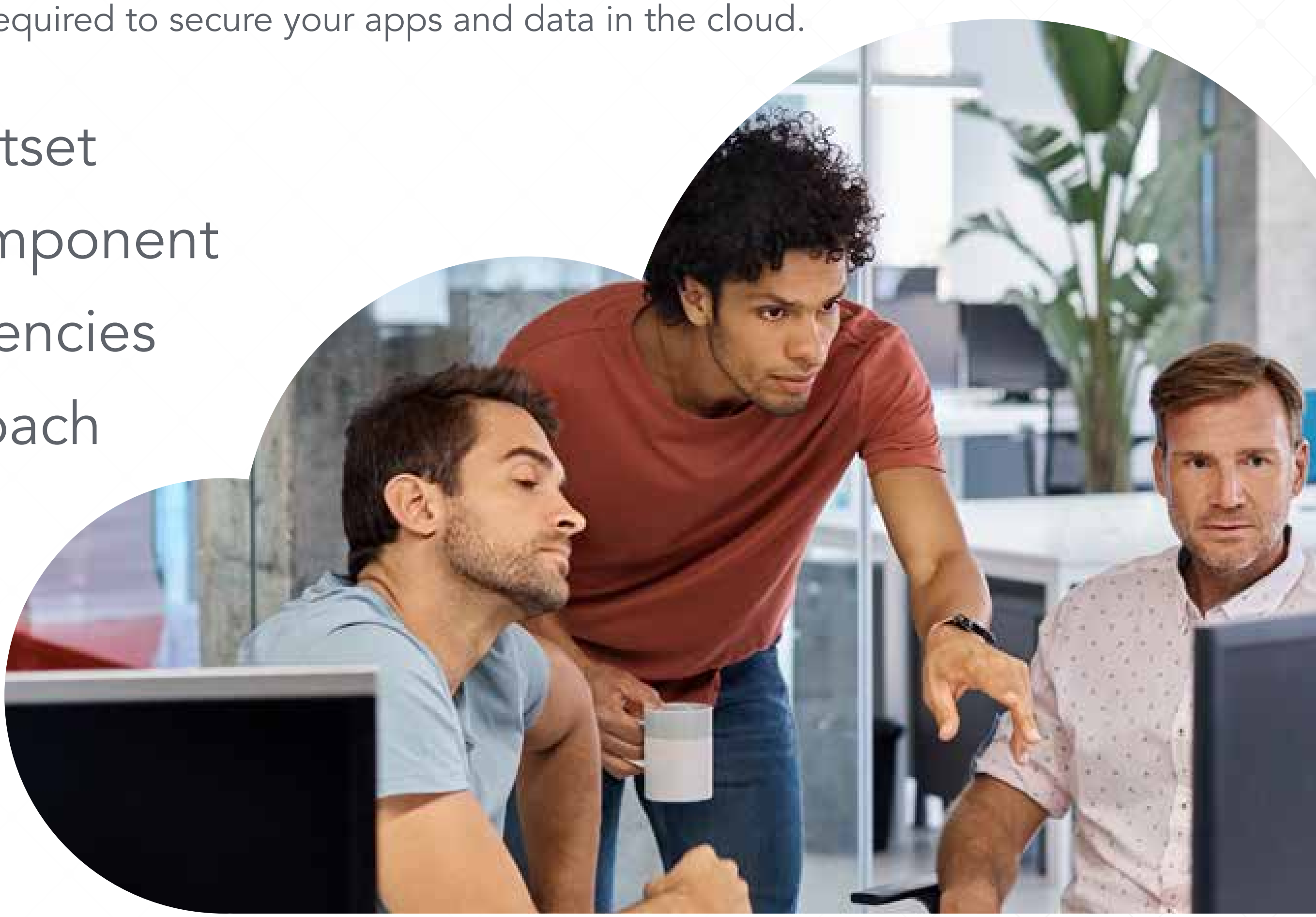
> *When migrating to the cloud, reassess and redesign security to meet the latest requirements and make the solution fit for modern integrations and cloud environments.*

Jonathan Bentley,
CISSP-ISSAP, CSSLP, CCSP,
Chief Enterprise Security Architect,
London, U.K.

Establish a Plan

Following the assessment of the on-premises infrastructure, businesses need to establish a solid plan to move securely to the cloud. Cloud security is always an ever thought and should be the foundation of every decision. With cloud security being a shared responsibility, assess the security solutions offered by cloud vendors, and select the controls required to secure your apps and data in the cloud.

- Security from the Outset
- Security in Every Component
- Understand Dependencies
- Take a Phased Approach



CCSP® Certified Cloud Security Professional

An (ISC)² Certification

Security from the Outset

Cloud security should be designed and implemented in your solution from day one. Evaluate the security protections offered by each cloud provider and always remember that the responsibility for protecting your data and applications in the cloud lies with you. Encryption, access controls, firewall configuration and API configuration should be considered in every cloud security migration strategy.

> *Bring security to the table from the very beginning and build security in by design, rather than retrofitting it at some later point which will cost more and may lead to disaster.*

David Hatter,
CISSP, CCSP, CSSLP,
Cybersecurity Consultant,
Ohio, U.S.A.

CCSP
Certified Cloud Security Professional
An (ISC)² Certification

Security in Every Component

Avoid vendor lock-in. Opt for multi-cloud architectures as cloud providers offer native security solutions that only work seamlessly in their own infrastructure and environment. Select a vendor-agnostic, cloud-based security solution to protect and monitor every component of the cloud.

Certified Cloud Security Professional

CCSP. An (ISC)² Certification

> *Whilst you may not have visibility of the complete migration, try and bake in as much security as possible into every cloud component from the get-go. Create an extensible cloud architecture that can accommodate a range of workloads without needing constant reworking, and can be re-deployed easily. Invest in cloud security monitoring, and incident response, and get eyes on glass for this, much of cloud is public by default. Don't forget, you still need to back up your data when using the cloud! Ensure that restores happen within business tolerance!*

Abhishek Vyas,
CISSP, CCSP,
Cloud Security Architect,
Cardiff, U.K.

Understand Dependencies

Your in-house applications and data have dependencies that need to be reviewed and understood. Communications and interfaces to other services and reliance on internal or external workflows need to be evaluated and redesigned for scalability in a cloud environment. Failure to do so may result in costly service breakdowns.

Certified Cloud Security Professional

CCSP®

An (ISC)² Certification

> *"Understand all dependencies and have an agreed upon list of minimum requirements. You need buy-in from your stakeholders and leadership more than ever because of how major a task migration can become."*

Fernando Deanda,
CISSP-ISSAP, ISSEP,
ISSMP, CCSP,
Risk Management Framework
SME & Infrastructure Manager
Texas, U.S.A.

Take a Phased Approach

Cloud migration is not a one-off exercise. It needs careful planning, with well-defined phases and expected outcomes. Establish measurable deliverables and closely monitor each migration phase to ensure requirements are met. Consult with your cloud provider's senior technical staff for the best approaches and always keep security at the forefront.

> *Plan the cloud migration in phases - embedding security controls right from the design stage and evaluate the migration strategy on an ongoing basis.*

Minghui Wu,
CISSP, CCSP,
Technology Audit Manager
Singapore

CCSP® Certified Cloud Security Professional
An (ISC)² Certification

Consider the Security Risks

As cloud environments blur traditional business boundaries and increase the threat landscape, organizations need to be aware of the impending risks. Configuration errors, weak identity and access management, poor authentication and authorization controls are credible risks that businesses need to address to reduce the impact of potential security incidents. With security in the cloud being the sole responsibility of the cloud customer, certified security professionals can bring invaluable knowledge to their organizations to effectively mitigate known (and unknown) risks and threats.

- Understand the Attack Surface
- Cloud Security is Unique – Rethink Processes
- Risks and Responsibility Remain
- Ensure Strong Encryption

CCSP® Certified Cloud Security Professional

An (ISC)² Certification

Understand the Attack Surface

Migration to the cloud will alter your threat surface. Corporate boundaries will blur and new risks and challenges will emerge. Failure to understand your attack surface will result in security oversight and gaps in policies and practices. Your security controls will also need to migrate to address new risk and compliance issues specific to the cloud.

> *"Understand your attack surfaces and risk tolerance level. On-premises and cloud are of different paradigms which justify different approaches in managing the resources securely.*

Si Wei Cheong,
CISSP, CCSP,
Cyber Security Analyst
Singapore

CCSP® Certified Cloud Security Professional
An (ISC)² Certification

Understand the Attack Surface

Migration to the cloud will alter your threat surface. Corporate boundaries will blur and new risks and challenges will emerge. Failure to understand your attack surface will result in security oversight and gaps in policies and practices. Your security controls will also need to migrate to address new risk and compliance issues specific to the cloud.

> *Refuse to rely on your understanding of on-prem security processes and procedures. Be willing to treat the cloud as unique, requiring unique processes and procedures.*

Vincent Romney,
CISSP, CCSP,
Enterprise Security Architect
Utah, U.S.A.

CCSP® Certified Cloud Security Professional
An (ISC)² Certification

Risks and Responsibility Remain

Data and application security in the cloud is the sole responsibility of the cloud customer. While the cloud provider assumes responsibility for the cloud, you are responsible for protecting your customers' data in the cloud. This is the foundational principle of cloud security. Failure to understand the Shared Responsibility Model results in costly data breaches.

Certified Cloud Security Professional
CCSP®
An (ISC)² Certification

> *No matter which cloud service provider you entrust with your data, services and/or infrastructure, ultimately you cannot transfer the risk and responsibility of protecting and securing your clients' and customers' data.*

Kimberley Dray,
CISSP, CCSP,
Senior Information Security Analyst,
Victoria, Canada

Ensure Strong Encryption

When it comes to data security in cloud environments, the key overriding principle is encrypt everything. We cannot stress enough the value of ensuring strong encryption of all corporate data in the cloud. This includes design and implementation measures to safeguard your encryption keys. A compromised key opens the door to your data.

> *Strong encryption must be applied to all data-at-rest and data-in-transit. If possible, adopt data-in-memory encryption in the cloud.*

Feng Wei Ni,
CISSP, CCSP,
Security Architect,
Toronto, Canada

Certified Cloud Security Professional
An (ISC)² Certification

Prepare and Maintain Compliance

GDPR, CCPA, HIPAA, PCI DSS and other sector-specific regulations mandate security and privacy requirements to safeguard sensitive and personal data, and ensure the reliable and safe delivery of critical services, such as energy, oil and gas, and transportation. Organizations need to have a thorough understanding of all regulatory requirements and be prepared to prove compliance. Accredited security professionals can act as trusted advisors to legal and executive staff because they understand how these requirements can be met without impacting the performance of cloud-based services.

- Responsibility Does Not Get Outsourced
- Get Guidance from Auditors
- Relevant Legislation at Storage Locations
- Assess the Need for New Controls

CCSP Certified Cloud Security Professional

An (ISC)² Certification

Responsibility Does Not Get Outsourced

Just like you are responsible for security in the cloud, you are also legally bound for mitigating the effects of a cloud-related data breach. You cannot outsource the impact of a data breach. Selecting the appropriate controls to protect and safeguard your applications, services and data in the cloud can help you minimize both the potential of a security incident and the impact of such an event.

Certified Cloud Security Professional

CCSP®

An (ISC)² Certification

> *Understand the roles and responsibilities of the enterprise vs. the Cloud Service Provider. So often I hear people state that something is not their problem since they are on a cloud provider's platform. That's simply not true and the enterprise gets burned when they later find out they are always ultimately the responsible party for their data.*

Tara Hunter,
CISSP, CCSP,
Senior Cloud Security Engineer,
Virginia, U.S.A.

Get Guidance from Auditors

If your organization is operating in a highly regulated environment such as the healthcare, finance or energy sectors, seek guidance and advice from your compliance auditors. They will be happy to assist you. A single cloud-related security incident affecting critical infrastructure might have a crippling effect or severely impact an organization.

Certified Cloud Security Professional

CCSP®

An (ISC)² Certification

> *If you are in a highly compliant environment, ask your auditors for very specific cloud requirements before you decide to move to the cloud. Don't forget to ask them for scenarios where cloud may cause a compliance violation.*

Adele Farhadian,
CISSP, CCSP,
Owner & Managing Director,
Vancouver, Canada

Relevant Legislation at Storage Locations

National and transnational privacy and security legislation, like GDPR or CCPA, have defined requirements for data portability and define protections for data residing in their territory. Cloud providers may store your data in physical locations different from your headquarters' location. Fully understand these security and privacy regulations to design your security policies and controls to ensure compliance and avoid costly penalties.

CCSP® Certified Cloud Security Professional
An (ISC)² Certification

> *Know where your provider will store data and the legal jurisdiction it falls under. You need to be aware and compliant with the regulations of both your own country and the jurisdictions where your data is physically stored.*

Charlie Platt,
CISSP-ISSMP, CCSP,
VP of Technology and Information Security,
Virginia, U.S.A.

Start with In-depth Analysis

Obtaining visibility into your organization's infrastructure, data and applications is the foundation of every security policy. You need to have a deep understanding of the application dependencies and perform a cost-based analysis to determine the real cost of upgrading to the cloud versus the expected added value.

> *Understand that when moving to the cloud, enhanced flexibility comes with more exposure to attack, and also a need for different controls. As you consider moving existing systems to the cloud, you need to evaluate whether the new controls, combined with the new risks, can be adequately addressed by the controls available to you in the new environment.*

Keith McMillan,
CISSP, CCSP,
Technical Fellow,
Wisconsin, U.S.A

CCSP®
Certified Cloud
Security Professional
An (ISC)² Certification

Prepare Your Team

The lack of appropriate training is a barrier to effective cloud security. In recent years, organizations have realized the power of having security teams that possess a foundational understanding of all things cloud – from initial planning and risk assessment to understanding compliance requirements to implement multi-cloud security. A security team with a multi-cloud skill set will help your business harness the power of the cloud without security headaches.

- Assess Roles and Responsibilities
- Create a Dedicated Cloud Team
- Robust Team Knowledge and Skills
- Provide Ongoing Training

CCSP® Certified Cloud Security Professional

An (ISC)² Certification

Assess Roles and Responsibilities

Agile and DevOps teams, the convergence of IT and Operational Technology (OT) and cyber-enabled Industrial Control Systems (ICS) require the shifting of the security mindset toward a holistic model, deeply integrated into organizations' workflows. Security risks in the cloud are operational risks and need to be addressed by all corporate stakeholders. This new mindset requires an assessment of current roles and responsibilities to make them consistent with flexible, scalable cloud environments. Security teams need to collaborate and work closely with all stakeholders to enforce a cloud-first security mindset.

> *"Strong partnership with security, application development and infrastructure teams is critical. Due to some of the security controls moving into a different OSI layer, different roles or jobs will need to assume responsibility for security control development, testing and adoption."*

Kris Boike,
CISSP, CCSP,
GRC Sr. Manager,
Minnesota, U.S.A.

CCSP® Certified Cloud Security Professional
An (ISC)² Certification

Create a Dedicated Cloud Team

A multidisciplinary cloud team will enable a smooth and secure transition from traditional business functions to cloud-enabled, flexible, scalable, secure and cost-effective operations. The team will oversee not only the initial migration to the cloud, but it will enable innovation and adoption of cutting-edge cloud solutions in close cooperation with the cloud providers' senior technical staff. Evolving together with technology will assure that organizations are always up to date, resilient and able to meet the shifting changes in the global environment.

Certified Cloud Security Professional
CCSP®
An (ISC)² Certification

> *Develop a cloud team. The team leads the company through organizational and business transformations over the course of the migration effort, and defines best practices, standards and drives change throughout the organization.*

Otto Lee,
CISSP, CCSP, CSSLP,
Security Assurance Lead,
Hong Kong

Robust Team Knowledge and Skills

You cannot have effective cloud security without the people required to enforce policies and practices. Security depends on people, processes and technology. Neglecting the "people" variable of the security equation will result in solutions that are neither fit-for-purpose nor user convenient. A robust and knowledgeable cloud security team will ensure the balance between security and user experience is maintained. Cloud security will become a competitive advantage, an enabler of innovation, fostering productivity and greater revenues.

Certified Cloud Security Professional
CCSP®
An (ISC)² Certification

> *Make sure you have enough security personnel who have robust knowledge and implementation skills of cloud security protection.*

Yiliang Zhou,
CISSP, CCSP,
Senior Cybersecurity Strategy Manager,
Shenzhen, China

Robust Team Knowledge and Skills

One of the barriers to effective cloud security is the lack of appropriate training. Organizations should invest in training all personnel regardless of their position. Understanding all components of cloud security and blending this knowledge with organization objectives and processes will enhance work performance and promote innovation. In addition, foundational knowledge about cloud infrastructure and security controls will eliminate costly configuration errors and minimize the impact of potential security incidents. An understanding of cloud security risks and challenges allows for realistic project management to migrate securely to the cloud.

Certified Cloud Security Professional

An (ISC)² Certification

> *Make sure you give your staff the appropriate amount of training and time to learn the technology. Some of the most disastrous cloud migrations I've seen were a result of not having the right staff involved in the migration.*

Keatron Evans,
CCSP,
Managing Partner,
Virginia, U.S.A

Conclusion

The journey to the cloud can become problematic if it does not come as a result of careful consideration and planning. Cloud security should be a constant consideration rather than an afterthought to help organizations reap the many benefits of the cloud.

Certified cloud security professionals have provided their valuable advice to help you navigate in safe waters, which is based on the technology, processes and people.

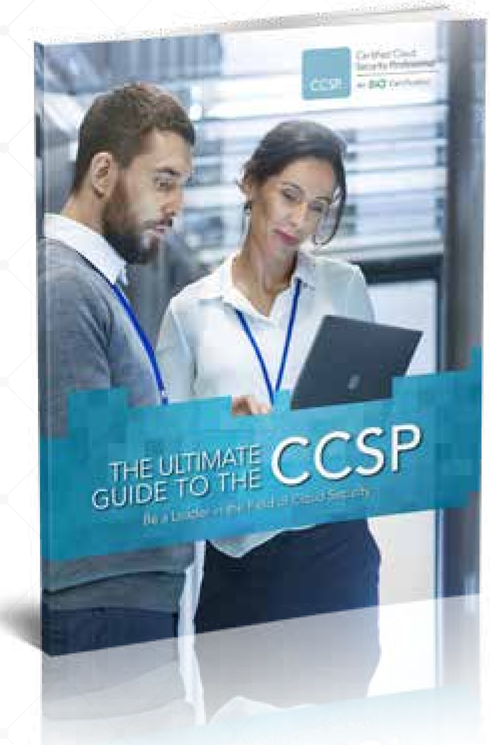
The (ISC)² Certified Cloud Security Professional (CCSP) certification is a market differentiator and has been ranked as the most valued cloud security certification and the third most valued security certification overall in 2020. The certification is vendor-neutral, and the acquired knowledge can be applied across a variety of cloud platforms, ensuring the ability to protect sensitive data in a global environment.

CCSP presents many advantages to all security professionals in whatever stage of their career, including credibility, unique recognition, enhanced knowledge and skill set, versatility, career advancement, and increased compensation.

CCSP complements vendor-specific training and demonstrates 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 the cybersecurity experts at (ISC)².

CCSP® Certified Cloud Security Professional
An (ISC)² Certification

Free Resources for Your Journey



CCSP

THE ULTIMATE GUIDE TO THE CCSP

Be a Leader in the Field of Cloud Security

Ultimate Guide to the CCSP

Get the Guide

CCSP

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

The Cloud Security Landscape

Take Your Cloud Security Career to Infinity (and Beyond)

Get the White Paper

CCSP

10 Reasons Why Businesses Need to Invest in Cloud Security Training

The cloud security landscape

Cloud security is a top concern

10 Reasons to Invest in Cloud Security Training

Get the White Paper

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 general public through our charitable foundation – The Center for Cyber Safety and Education™.

For more information on (ISC)^{2}, visit **isc2.org** follow us on **Twitter** or connect with us on **Facebook** and **LinkedIn**.