CCSP®

# 10 Reasons Why Businesses Need to Invest in Cloud Security Training

## The cloud security landscape

Companies are increasingly migrating data, applications and services from on-premises data centers to the cloud, seeking to innovate, disrupt their markets and reap the benefits the cloud is delivering: flexible capacity and scalability, improved availability and increased agility.

The migration process to the cloud is not without concerns. In fact, it is a balancing exercise, where businesses need to plan and decide the most effective migration scenarios. Many businesses have opted into migrating data and services to multiple cloud environments to avoid vendor lock-in. A recent report by Thales[1] indicates that 98% of global organizations store some kind of sensitive data in the cloud, while 95% of the survey respondents use SaaS applications, 67% IaaS platforms and 65% PaaS environments. Further, other businesses decide to create a hybrid computing environment and maintain some legacy applications and data on-premises because it is not feasible to move them to the cloud.

## Cloud security is a top concern

Despite the many advantages that cloud environments offer, organizations are facing new challenges and concerns. Amongst those, cloud security is ranked as a key issue for cloud customers[2]. Cloud adoption blurs traditional corporate boundaries and renders traditional security controls inappropriate. Most legacy security tools are not designed for the dynamic, distributed, virtual environments of the cloud. As a result, 82% of the Cloud Security 2020 survey[3] 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 and threats which bad-actors are eager to exploit. The most common attack vectors in the cloud are misconfiguration of the cloud platform (68%), unauthorized access (58%), insecure interfaces (52%), and hijacking of accounts (50%). The Thales Data Threat 2020 report[4] indicates that 49% of global respondents experiencing a breach affecting data in the cloud.

With more cyberattacks targeting cloud workloads, organizations are becoming less confident about their cloud security posture. Security needs to evolve to allow for flexibility while securing the ever-expanding threat landscape inherent in multi-cloud and hybrid environments. Organizations need to ensure a holistic and effective approach to cloud security. To successfully protect themselves, businesses need to rethink security which should be inclusive of all cloud components: data, users, apps, and infrastructure.

Adoption of effective cloud security does not come without barriers. Complexity is a significant factor to consider which is self-inflicted by the dominance of multi-cloud environments. The 2020 Cloud Security Report revealed that the biggest challenge organizations are facing is the lack of staff expertise and training. According to Global Knowledge[5], nearly 80 percent of IT decision-makers say their teams lack the skills they need. And this challenge is particularly acute when it comes to cloud computing. In fact, a report from 451 Research[6] indicates that cloud skills gaps have nearly doubled in the past three years, with 90 percent of organizations reporting shortages.

These statistics come as no surprise to business leaders around the world who are struggling to find talented developers, architects, and senior management to help them make the most of the cloud. There are simply not enough highly experienced applicants to meet the demand. CISOs are faced with the task of strengthening the cloud security posture with the available staff and financial resources, not easy considering the skills gap, time constraints and difficulty of hiring experienced security professionals. In addition, they need to come up with incentives to retain the existing, experienced security team members. Cloud security should become an integral part of the corporate culture, where everyone, depending on their position, will have certain roles and responsibilities to fulfill.

| **CISO Challenges** | **Entry-level** | **Junior Management** | **Senior Management** |
|---|---|---|---|
| Retention | ✓ | ✓ | |
| Apply cloud security principles | ✓ | | |
| Enforce security strategies | ✓ | | |
| Motive for career success | ✓ | | |
| Align business with security | | ✓ | |
| Enabler of innovation | | ✓ | |
| Foster increased productivity | | ✓ | |
| Stand out of competition | | ✓ | |
| Develop cloud-first strategies | | | ✓ |
| Drive innovation | | | ✓ |
| Increase business revenue | | | ✓ |
| Lead to the future | | | ✓ |
| Mentor the younger generation | | | ✓ |
| Promote security culture | | | ✓ |

*Figure 1: CISO challenges for strengthening the cloud security posture.*

## The benefits of investing in cloud security training

With the increasing emphasis on remote work, cloud security has become the #1 skill and the most desired area in continuous professional development[7]. Recent surveys indicate that training and certifying IT staff on cloud security is the primary tactic organizations deploy to assure their evolving security needs are met. Interestingly, 80% of professionals admit that they and their teams need cloud security training or certification to be better equipped to operate in cloud environments[8]. This rate will continue to grow rapidly as organizations turn to vendor neutral cloud-based security solutions versus on-premises legacy ones. Rather than chasing and competing for a limited number of highly experienced professionals, businesses should empower their employees with strong foundational cloud skills.

Modern businesses are faced with so many challenges while moving to the cloud that investing in cloud security training is a critical business decision. Here are ten reasons why businesses need to consider investing in cloud security training.

***1. Minimize the impact of a security event***

The damages that follow a cyber-related incident can be expensive and detrimental for business. Thus, the benefits of investing in cloud security awareness training outweigh the cost of a leak or breach. The following are some of the potential repercussions should your business fall victim to a cyber-attack:

- » Loss of revenue
- » Reputation damage
- » Loss of clients
- » Operational disruptions
- » Lawsuits

- Intellectual property (IP) cyber theft
- Theft of personally identifiable information (PII)
- Compromised client data, sensitive business information and equipment

***2. Build a culture of security***

A comprehensive cloud security awareness program sets clear expectations for all employees and educates users about how to recognize attack vectors, help prevent cyber-related incidents and respond to a potential threat. Training employees about safe online computing, strong authentication, social engineering and more, will transform your staff into your first line of cyber defense and ensure the confidentiality of sensitive business data.

***3. Ensure business resiliency***

By building strong, knowledgeable, and resilient teams that do not depend on a small number of irreplaceable employees, you can help ensure business continuity and financial stability. Educating individuals with a range of skills on cloud security will also have a positive impact on business decision-making and innovation.

***4. Meet the challenge of regulatory compliance***

Businesses operate under certain regulatory environments. While there are industry specific standards and regulations, like the PCI DSS or HIPAA, that dictate how these organizations should protect sensitive data, there are also cross-industry, national or transnational regulations that safeguard the confidentiality and integrity of personal data. Regulations like the GDPR or the CCPA have strict data security requirements and provision huge fines in case of data breaches.

Training your security teams about these requirements, you will empower them to maintain regulatory compliance in cloud environments. Being aware of this legal background can help them configure cloud platforms and select the controls appropriate for safeguarding their assets in the cloud.

***5. Accelerate innovation***

Cloud security expertise is becoming increasingly valuable for businesses. The vast majority of companies are expected to expand their cloud services in the next one to three years[9], a testament to the benefits of cloud adoption. In the midst of this rapid acceleration, IT leaders recognize the importance of retaining employees who fully understand the complex and quickly changing cloud environments, because their organization will function more effectively with a uniformly shared foundation of cloud security knowledge. This education additionally benefits the time-to-value for new products and features, which is accelerated by investing in the cloud.

***6. Strengthen employee retention***

Not only does an investment in cloud learning provide benefits for enterprise operations, it also leads to enhanced career development opportunities for employees, creating greater workplace satisfaction and retention. Employees are more likely to stay long term with an employer who invests in their career through skills development, cementing that additional training has a big impact on employee happiness.

By surrounding your experienced cloud staff with skilled, enthusiastic employees who are early in their career, you will free them to take on the high value facets of projects. They can do initial planning, and then focus on more complex tasks, such as strategy and design. This is an advantage not only for the employees, but for the organization, because as employees' tasks are more aligned to their abilities, they will stick around longer. In a 2020 survey by Deloitte[10], respondents who said their companies use their skills effectively are more likely to say they plan to stay with their current employer.

***7. Foster confidence, minimize stress***

Studies and reports[11] indicate that security teams are overwhelmed by the sheer amount of security incidents they need to mitigate daily, and they even feel stressed by data breach news. Keeping employees abreast of the latest threat intelligence and attack methods in the cloud will help mitigate the anxiety caused by cybersecurity uncertainty. In addition to reducing stress, security training helps minimize risky actions and instill security best practices company wide. By accentuating cloud security as a priority for your company, employees are provided with the advanced tools and resources needed for adequate training. Furthermore, it enables shared responsibility among staff for safe technology usage.

### *8. Save time and resources*

Skills gaps are more than just an inconvenience; the financial and business repercussions can be grave. The IDC anticipates[12] that in 2020, "90 percent of all organizations will have adjusted project plans, delayed product/service releases, incurred costs or lost revenue because of a lack of IT skills." By upskilling entry-level staff, you can bridge your IT skills gap, helping your company achieve its business objectives and meet demands on time.

Advancing the knowledge on cloud security for junior employees is critical especially for small and medium businesses that cannot afford to hire experienced professionals. Rather than hiring for hard-to-find technical skills alone, enhancing the knowledge base of entry-level practitioners with technical aptitude, potential, and enthusiasm is a great investment for the future of the company.

### *9. Customer satisfaction*

A data breach can cause reputational damage and dissolve any confidence that customers may have had in a company, while others might pursue legal repercussions to impose further damage. By investing in innovative, comprehensive cloud security training to educate staff, customers can find ease in knowing that their data in a cloud-based application are stored and/or processed by a company that places security as a top priority.

### *10. Stand out of competition and secure long-term success*

With businesses moving to multiple cloud platforms, upskilling your staff in cloud security can help them navigate safely between all cloud platforms. Provisioning of a multi-cloud knowledge ensures that your company remains agile and can easily adapt to changes in the industry.

Cloud security training should not focus solely on IT teams. Enterprise leaders should plan to include cloud learning in their budget and employee development plans. There should be a cadence for training—either monthly, quarterly or aligned with annual performance reviews—to integrate this ongoing learning into the existing HR program. HR teams who prioritize upskilling will be building a highly trained and incredibly adaptable workforce.

By investing in cloud security awareness training, you are investing in the future of your company.

## Considerations for selecting a cloud security training provider

With so many benefits presented by investing in cloud security training, the challenge now is to select the provider who will satisfy all your needs.

***Foundational knowledge and skills***

The need for skills and foundational knowledge of cloud security is underpinned by the fact that cloud security functions is a shared responsibility between the cloud providers and the business customers using them. Major cloud vendors, such as AWS[13], Azure[14], or Google Cloud[15] 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 corporate data they store on cloud platforms, their applications and operating system, 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 the access to corporate resources, and for the encryption of the data at rest and in transit.

To meet the foundational requirements of the shared responsibility model, the candidate cloud security program should provide a solid knowledge of the cloud security and design principles, such as cryptography, access control, virtualization security, and vendor lock-in. Further, it needs to empower employees with the knowledge 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 knowledge base of the cloud security training program should also cover all aspects of risk assessment and threat mitigation, as well as software assurance and security in the cloud and supply chain challenges.

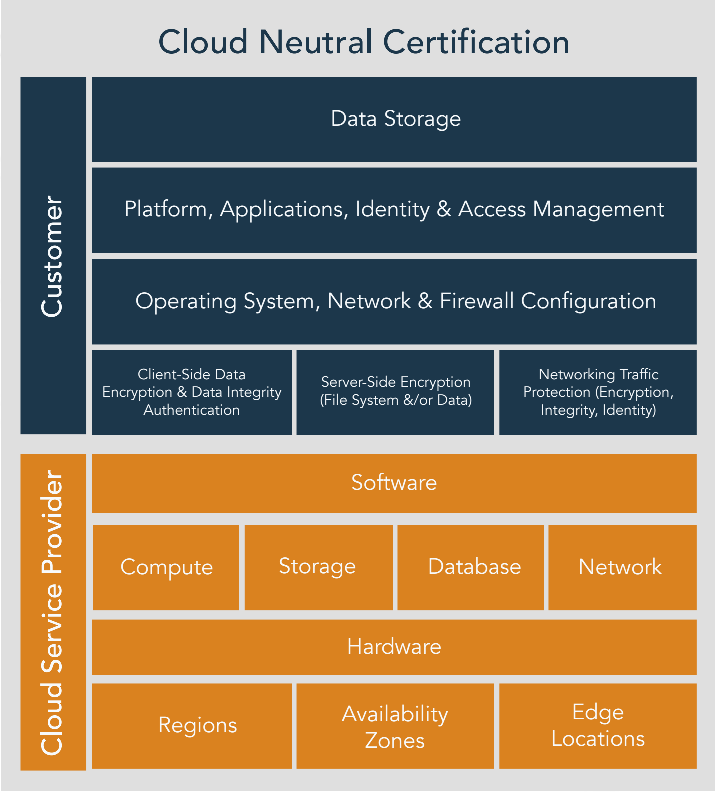
Cloud Neutral Certification
Customer
Data Storage
Platform, Applications, Identity & Access Management
Operating System, Network & Firewall Configuration
Client-Side Data Encryption & Data Integrity Authentication
Server-Side Encryption (File System &/or Data)
Networking Traffic Protection (Encryption, Integrity, Identity)
Cloud Service Provider
Software
Compute
Storage
Database
Network
Hardware
Regions
Availability Zones
Edge Locations

*Figure 2: The Shared Responsibility Model.*

## Vendor neutrality

With businesses opting for multi-cloud environments and vendor neutral cloud security solutions, the neutrality of the certification is a huge bonus for businesses seeking to protect their multiple and/or hybrid cloud environments. Vendor native training offered by cloud providers focuses on the operational knowledge you need to configure the platform and avoid costly mistakes. This kind of hands-on training limits the scope and the applicability of the knowledge gained.

On the other hand, a vendor neutral certification broadens this operational knowledge and provides you with the big picture about cloud computing and security. A vendor-agnostic cloud certification can help you understand concepts like legal compliance, roles and responsibilities, alignment of security objectives with business goals.

The knowledge acquired through a neutral certification coupled with the personnel's background and experience can greatly enhance the corporate cloud security posture. Before selecting a provider for your cloud security training, you must thoroughly examine their knowledge base and their offerings. Ensure that the knowledge gained can give your business a great return on the investment and can help you secure your cloud solutions.

## Benefits of CCSP

***Command the Cloud with CCSP***

While there are many cloud security certifications on the market, the (ISC)$^2$ Certified Cloud Security Professional (CCSP) is the certification that can significantly enhance your corporate cloud security posture. CCSP is a global standard and recognized as the most valued cloud security certification and the third most valued security certification overall in 2020[16].

The CCSP certification knowledge base is authoritative and exemplifies the commanding leadership essential for ensuring that cloud security is holistically incorporated into every cloud solution. Enforcing a corporate wide cloud security mindset is achieved by utilizing a vast knowledge base and a disciplined skillset.

CCSP is a vendor-agnostic certification which ensures that security teams' members can perform cloud security in multi-cloud or hybrid environments. With businesses seeking to avoid vendor lock-in and utilizing a multitude of platforms and solutions, the neutrality of CCSP certification is a great bonus for businesses looking to apply effective controls, policies, and configuration best practices over a variety of platforms.

The CCSP certification is identified as the premier cloud security qualification because of its unique criteria. The certification is recognized as a market differentiator, offering unsurmountable advantages when compared to other equivalent certifications. The certification introduces many benefits and holding it presents many advantages in an increasingly competitive landscape.

***Benefits at any stage of career***

Cloud security is not the responsibility of just the security teams. Every employee has a role to play in keeping data safe. To do so, they need to have a solid understanding of cloud computing and the security risks and challenges associated with the cloud. They also need to be educated about what their role will be in protecting corporate data in the cloud.

By incorporating data security training into the on-boarding process and regular training protocols, the organization will be able to develop and maintain a mindset where cloud security is an ever thought, to become much safer from cyber threats.

The knowledge and skills earned by taking the CCSP exam are important for all employees irrespectively of their age or position and can help them meet the expectations set by the business executives. Cloud computing is such an integral part of business operations, the structured and disciplined knowledge earned while pursuing the CCSP certification can only enhance your business security posture.

***Entry-level***

Cloud security training and certification for entry-level employees is a great investment. CCSP can help them leverage the hands-on training offered by the various cloud providers and apply it to both multi-cloud and hybrid environments. They will become a valuable asset to your CISO as they will be able to translate and implement effectively cloud security policies into well-established, robust practices and solutions to protect the corporate data from the preying eyes of cyber criminals. The certification can also help them become an integral part of the organization's journey to the cloud, developing a sense of ownership and serving as a great motive for further success.

***Junior management***

On the other hand, mid-management employees will gain from participating in the CCSP exam by complementing their business experience with technical foundational knowledge about the risks and challenges of cloud computing. They will have a wider understanding of how cloud risks can impact operational reliability and stability and may become an enterprise-wide risk. They can become valuable advisors to senior executives, aligning business objectives with security goals and contributing to defense in depth. Eventually, they will become enablers of innovation, increased productivity and success.

***Senior management***

Finally, senior management executives can benefit from the foundational knowledge gained from participating in the CCSP certification by helping them to develop strategies to drive the business journey to innovation and success. Understanding how secure cloud computing can propel organizations to increase business revenue will assist them to make the right decisions and lead their company into the future. In addition, they can become the mentors of the younger generation, with their organizational wisdom becoming a beacon of inspiration.

## How CCSPs Give Organizations a Competitive Advantage

CCSP is an essential partner for your organization to excel in cloud security. Earning the globally recognized CCSP cloud security certification is a proven way to better secure critical assets in the cloud. The CCSP shows that your employees have the technical skills and knowledge to manage and secure data, applications and infrastructure in the cloud using best practices, policies and procedures established by the cybersecurity experts at (ISC)².

The CCSP is the start of your organization's journey to cloud computing. By earning Continuing Professional Education (CPE) credits, you can ensure that the continuous professional development of your employees evolves along with cloud technology. The structured knowledge earned by holding the CCSP certification can benefit your business in multiple ways and is a sure investment into securing your organization's future success in a shifting global environment.
Your organization can benefit from both available learning options – individual or in-house team training. (ISC)² offers a tailored training solution centered around your organization's cybersecurity certification needs and requirements. Whether you have a global workforce that requires varied training options or a smaller staff that needs a private training seminar at one central location, (ISC)² delivers a solution that fits your budget, schedule, and certification objectives.

(ISC)² is the leader in security certifications and is acknowledged by companies worldwide. To learn how your business can benefit, check out our Enterprise Training Solutions https://www.isc2.org/Training/Enterprise-Solutions.

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

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

[5] Global Knowledge, 2020 IT Skills and Salary Report, available at https://www.globalknowledge.com/us-en/content/salary-report/it-skills-and-salary-report/

[6] Virustream, Demystifying cloud transformation: Where enterprises should start, available at https://www.virtustream.com/lp/451-research-cloud-transformation

[7] (ISC)$^2$ 2020 Cybersecurity Workforce Study https://www.isc2.org/Research/Workforce-Study

[8] SecurityScorecard, CyberEdge, 'The Impact of COVID-19 on Enterprise IT Security Teams' Report, available at https://securityscorecard.com/resources/impact-of-covid-19-on-enterprise-it-security-teams

[9] A Cloud Guru, State of Cloud Learning Report 2020, available at https://go.acloudguru.com/2020-state-of-cloud-learning-report

[10] Deloitte University Press, Surveying the Talent Paradox from  the Employee Perspective, available at https://www.deloitte.com/content/dam/Deloitte/mx/Documents/about-deloitte/Talent2020_Employee-Perspective.pdf

[11] Sophos, The Impossible Puzzle of Cybersecurity, available at https://secure2.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-impossible-puzzle-of-cybersecurity-wp.pdf

[12] IDC, 2020 IT Training Buyer Survey Spotlight: Impact of Skills Gap and the Need for Strategic IT Skills Development, available at https://www.idc.com/getdoc.jsp?containerId=US46269520

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

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

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

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