LDR520: **Cloud Security for Leaders™**

5 Day Course	30 CPEs	Laptop Required

You Will Be Able To

- Define a strategy for securing a workload in the cloud for medium and large enterprises that can support their business objectives
- Establish a security roadmap based on the security strategy that can support a fast-paced cloud adoption and migration path while maintaining a high degree of security assurance
- Understand the security fundamentals of the cloud environment across different types of service offerings, then explain and justify to other stakeholders the relevant strategic decisions
- Build an effective plan to mature a cloud security posture over time, leveraging security capabilities offered by cloud providers to leapfrog in security capabilities
- Explain the security vision of the organization in the Cloud domain to your Board Directors and executives, collaborate with your peers, and engage your workforce, driving the security culture change required for the cloud transformation

> **"Team is collaborative. We are all able to bounce ideas off of each other comfortably and using AWS to get hands-on makes it feel more real than if we were answering questions on a quiz."**
>
> —Richard Sanders,
> **Best Western International**

Strategically maximize your cloud investment.

Cloud Security Strategy is a comprehensive plan to protect the organization's data, workload, and infrastructure residing in the cloud(s) environment.

Cloud adoption is popular across all types of industries, and many organizations are taking strategic advantage of the cost and speed benefits of transitioning to the cloud. Since cloud environments differ significantly from traditional on-premises IT environments, in terms of protection requirements and threat vectors, the traditional network perimeter is no longer the most effective defense in cloud solutions. Organizations are migrating mission-critical workloads and sensitive data to private and public cloud solutions without always understanding the numerous key decisions needed for an organization's successful cloud transition. This cloud security implementation course walks the audience through the journey to mature their cloud security in each of the relevant security domains of could security strategy from beginning to high maturity state.

LDR520 complements traditional IT management techniques that leaders are accustomed to and helps with making appropriately informed decisions around strategy, financial investment, and necessary team technical knowledge and skill. We cover the key objectives of security controls in the cloud environment, including planning, deploying, and running the environment from the starting point to a progressively more mature state. There will be a focus on locking down the environment, securing the data, maintaining compliance, enhancing security visibility to the operations, and managing the security response on a continuous basis. Students will learn the essentials to lead the security effort for the cloud transition journey.

Business Takeaways:

- Establish cloud security program supporting the fast pace business transformation
- Understand current and future maturity level of the cloud security in contrast to the industry benchmarks
- Make informed decisions on cloud security program
- Anticipate the security capabilities and guardrails to secure the cloud environment
- Safeguard the enterprise data as workloads are migrated to the cloud

Hands-On Cloud Security Strategy Training

LDR520 uses case scenarios, group discussions, team-based security leadership simulations with embedded real life technical components to help students absorb both technical and management topics. About 60 minutes per day is dedicated to these learning experiences using the Cyber42 leadership simulation game. This web application-based game is a continuous exercise where students play to improve security culture, manage budget and schedule, and improve security capabilities at a fictional organization. This puts you in real-world scenarios that spur discussion and critical thinking of situations that you will encounter at work.

sans.org/LDR520

- **Watch a preview of this course**
- **Discover how to take this course: Online, In-Person**

Section Descriptions

SECTION 1: Cloud Security Fundamentals and Identity Management

The first section of the course aims to help management professionals develop a solid fundamental knowledge into cloud adoption models and gain understanding on one of the most important security domain within cloud security which is Identity and Access Management (IAM).

TOPICS: Introduction to Cloud; Cloud Service Model; Transition Process; IAM – Segregation; IAM – Identity Management; IAM – Access Management

SECTION 3: Data Protection, Security Detection and Response

In Section 3, we delve into three key cloud security domains: data asset protection, security detection and response in the cloud environment, and governance aspects of cloud security.

TOPICS: Data Encryption and Key Management; Data Classification and Protection; Data Backup; Security Intelligence; Security Detection Analysis and Monitoring; Security Response and Transformation; Log Management; Security Governance Committee; Security Policy; Cost Management

SECTION 5: Multicloud and Capstone Exercise

In Section 5, we delve into the growing trend of adopting multi-cloud systems and emphasize the significance of a security strategy tailored for multi-cloud environments. Additionally, we examine the management aspects of the Software as a Service (SaaS) model and its application in enterprise settings. The section concludes with a capstone exercise, allowing students to apply the concepts, management tools, and methodologies they have learned in a practical scenario.

TOPICS: Multicloud Management; Program Roadmap and Transformation Planning

SECTION 2: Cloud Security Environment Protection and Architecture

The second section of the course is dedicated to managing the technology aspect of the cloud environment. Securing cloud technology is rather different than securing technologies on-premise. This section will highlight the difference and discuss the capabilities and competencies that matter the most.

TOPICS: Config Management; Image Management; Resource Management; Network Management; Cloud Architecture

SECTION 4: Securing Workload and Security Assurance

Section 4 begins with a focus on securing applications/workloads within the cloud environment. The discussion then transitions to security assurance, followed by an exploration of workforce transformation required to support cloud security transformation.

TOPICS: Cloud Application Practices; Application Assessment; Security Protection Services; Posture Validation; Regulatory Compliance; Security Testing; Skill Readiness; Organizational Alignment

> **"I recommend this course thanks to the multi-cloud approach and cloud-agnostic strategy, where we learned to consider and ask the right questions related to the cybersecurity part."**
>
> —Madjid Kazi Tanoi

> **"Great way to break out of just the technical aspects of cloud and a step towards management-level learning."**
>
> —Joshua Rosetta, **Penn State Health**

Who Should Attend

The primary target audience for this course is managers and directors who are in a position to lead or make key decisions on the IT transformation to cloud environments.

NICE Framework Work Roles

- Information Systems Security Manager (OPM 722)
- Program Manager (OPM 801)
- IT Project Manager (OPM 802)

Prerequisites

Students should have three to five years of experience in IT and/or cybersecurity. This course covers the core areas of security leadership in migrating workloads to the cloud environment and assumes a basic understanding of technology, networks, and security.

Notice to Students

This course will have limited overlap with the SANS SEC488: Cloud Security Essentials course because it will provide foundational information on cloud services and cloud security to ensure that students are on the same page.

> **"I loved the labs. They really helped emphasize what we are learning."**
>
> —Jana Laney