MGT520: **Leading Cloud Security Design and Implementation**

3 Day Course	18 CPEs	Laptop Required

You Will Be Able To

- Define a strategy for securing a workload in the cloud for medium-size 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 basics of the cloud environment across different types of service offerings, then explain and justify to other stakeholders the decisions within the security roadmap
- 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

"This type of training, i.e., cloud security from a management perspective, is rare and the quality of this one is definitely amazing."

—Benoit Ramillon, **UEFA**

Building and Leading a Cloud Security Program

Cloud adoption is popular across all types of industry, and many organizations are taking strategic advantage of the cost and speed benefits of transitioning to the cloud. Organizations are migrating mission-critical workloads and sensitive data to private and public cloud solutions. However, an organization 's cloud transition requires numerous key decisions.

This course focuses on what managers, directors, and security leaders need to know to develop their cloud security roadmap, to manage the implementation of cloud security capabilities. Making the right security decisions when adopting the cloud requires understanding the technology, process, and people related to the cloud environment. This complements traditional IT management techniques that managers are accustomed to and helps with making the appropriate informed decisions. We will 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
- Make informed decisions on cloud security program
- Anticipate the security capabilities and guardrails to build for the securing the cloud environment
- Safeguard the enterprise data as workloads are migrated to the cloud

Author Statement

"Cloud transition is common in many organizations these days, but many security leaders feel overwhelmed and underprepared for the security aspects of the cloud. When organizations accept security as an integral part of the transformation path, they can not only achieve the same level of security as their in-house IT environment, but also take advantage of a huge opportunity to leapfrog in security using cloud capabilities. In MGT520, we discuss industry-proven techniques to plan for the security aspects of cloud transformation. This course will arm students with the necessary information to confidently lead their organization towards securing the cloud workload and leveraging cloud capabilities to further enhance their security maturity in the IT environment."

—Jason Lam

Section Descriptions

SECTION 1: Security Program Design, Governance, and Identity Management

The first section of the course aims to help management professionals develop a migration roadmap to the cloud environment. The goal of the roadmap is to support the business transformation to realize the benefits from the cloud, while maintaining the security of the environment, applications, and data. We will arm you with information on various approaches to migratory and preparatory steps to get you ready for a secure migration journey.

We will then pivot over to the topic of security governance to provide the details to help you understand how to build up security governance in enterprise context. Not only do we provide you with the best practices in the governance area, we also provide the progressive approaches to build up security maturity as well.

We end the section covering a new security perimeter paradigm - the Identity and Access Management. With the modern Cloud architecture, we are losing the firewall and network perimeter as our main battle line. The transition from network centric to identity centric security perimeter requires a fundamentally different culture and mindset to effective management. We cover the key objectives and the common paths to gain security maturity.

TOPICS: Introduction to Cloud; Transition Process and Planning; Security Governance; Identity Access Management

SECTION 2: Cloud Technical Protection and Monitoring

The second section 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.

Students will learn about secure infrastructure and architecture first which includes key topics such as configuration management, resource management, and network controls. Students will learn how to lead their respective organization on driving iterative improvements in these domains over time which helps to improve defenses over time.

We then pivot into the security detection and response area. Students will learn the modern approaches to monitor for security events and respond to security incidents across the cloud and on-premise environment. We cover the modern approaches to progressively automate the processes so the monitoring can be as efficient and effective as possible.

TOPICS: Secure Infrastructure and Architecture; Security Detection and Response; Data Protection

SECTION 3: Securing Workload and Security Assurance

Section three starts off with covering the effort and key decisions related to securing the workloads in the Cloud environment. As organizations are moving their entire development pipeline to the Cloud environment, there are numerous key security decisions that need to be made.

Organizations are often challenged with the question of whether the cloud environment is meeting up to the security expectations, and whether it has vulnerabilities. The material on security assurance helps students to lead the building a security assurance program for cloud environment using automation as a basis of operations.

Multicloud is a natural progression to Cloud adoption. We cover the necessary management principles to successfully navigate through the complex security management of a multi-cloud environment.

Cloud adoption is a long-term process. We arm you with the information to drive the changes required by measuring the cloud security posture and using metrics to aid in making the right decisions.

TOPICS: Securing Application/Workload; Security Assurance; Workforce Transformation; Multi-cloud management

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: OV-MGT-001
- Executive Cyber Leadership: OV-EXL-001
- Program Manager: OV-PMA-001
- IT Project Manager: OV-PMA-002
- Cyber Intel Planner: CO-OPL-001

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. This course focuses on what managers, directors, and security leaders need to know about developing their cloud security plan/roadmap and managing implementation of cloud security capabilities.

"I feel like there was a lot of valuable material and would be very relevant for people creating a cloud security program."

—Jeff Henderson