Specialization Syllabus Submission

Specialization Overview

Specialization Title: *Cybersecurity in the Cloud*
Partner Name: *University of Minnesota*
Corresponding Competency Area from Coursera's Career Track Content List (ignore if not creating Career Track content):
Will this Specialization have a Culminating Project as the final course? *No*

Executive Summary: *What will a learner be able to do after completing this Specialization?*

A learner with no previous experience should be able to select an appropriate set of basic cybersecurity measures to protect an example cloud application. The learner should also be albe to identify the authorities (organizations, enterprises, and their officials) that typically have legal or contractual responsibilities for securely implementing an example cloud application.

Course 1

Course Title: *Basics of Cybersecurity in the Cloud*
Corresponding Topic(s) from Coursera's Career Track Content List (ignore if not creating Career Track content)**:**
Course Project

- **Title: Security Plan**
- **Type: Peer Reviewed**
- **Prompt:** *For this project, you will create a Security Plan for an example application implemented in the cloud using Software as a Service. The plan should identify the security responsiblities of all service providers and indicate which security measures are provided by which providers.*
- **Artifact:** *Through the project, learners will perform a high-level risk assessment, design a basic security system to address the risks, and identify parties responsible for different cybersecurity roles.*

Course Learning Objectives: (3+ per course)
"After completing this course, a learner will be able to..."

- *Given a scenario for migrating from privately-owned servers to cloud servers, identify key security risks to be addressed.*
- *Given a set of security risks in a cloud implementation scenario, select appropriate security measures to address them.*

- *Given a selected cloud service model and deployment model, identify the actor (consumer or service provider) responsible for implementing the different security measures.*
- *Given a selected cloud service model and deployment model, identify the trust boundaries that separate the cloud consumer, the end users, and the cloud service providers.*
- *Identify typical legal and contractual sources of cloud auditing and event logging requirements.*

Course 2

Course Title: *Data Security for the Cloud*
Corresponding Topic(s) from Coursera's Career Track Content List: (ignore if not creating Career Track content)
Course Project:

- **Title: Data Distribution Plan**
- **Type: Peer Reviewed**
- **Prompt:** *For this project you will write a Data Distribution Plan. We have an application that involves two or more classifications of data (TBD). The end user interface needs to provide an integrated display to allow navigation and updating of this data. Distribute the application's data items among cloud services to enforce "least privilege" and "separation of duty." Identify security measures to keep the separate cloud services separate.*
- **Artifact:** *Through the project, learners will distribute data among cloud services to minimize the risk of spillage to unauthorized users.*

Course Learning Objectives: (3+ per course)
"In this course, a learner will be able to…"

- *Give examples of how different phases of the cloud data life cycle are affected when handling data with different classifications.*
- *Given a set of data classifications and user roles, describe a set of access controls that yields "least privilege."*
- *Describe strategies for reducing the attack surface of consumer data at a cloud data center from the cloud service provider.*
- *Identify different strategies used to protect data in cloud applications and how they relate to cloud service providers, consumers, carriers, and end users.*
- *A flaw in a cloud application has disclosed customer data. Given the high-level features of the application, identify the types of legal and contractual liabilities faced by the following: the developers, their managers, their company's senior management, the company's customers, and the cloud provider.*

Course 3

Course Title: *Application Security for the Cloud*
Corresponding Topic(s) from Coursera's Career Track Content List: (ignore if not creating Career Track content)
Course Project:

- **Title: Key Management Plan**
- **Type: Peer Reviewed**
- **Prompt:** *For this project you will write a Key Management Plan for an example application implemented in the cloud using Infrastructure as a Service. The application will handle personally identifiable information about end users, but will not handle financial information. Identify which service providers are responsible for, or have custody of, the necessary cryptographic keys. Take reasonable steps to enforce Least Privilege on the keys.*
- **Artifact:** *Through the project, learners will select cryptographic measures for a cloud application and associate the corresponding crypto keys logically and physically with elements of the system.*

Course Learning Objectives: **(3+ per course)**
"In this course, a learner will be able to…"

- *List and describe the OWASP Top 10 vulnerabilities.*
- *Identify methods to provide cloud security assurance as part of the development life cycle, e.g. in a continuous delivery environment.*
- *List and describe the different types of virtualization or sandboxing used to protect cloud applications at either the server or client.*
- *Describe the application of authentication factors and federated identity solutions in cloud client and server authentication.*
- *Given a cloud application, explain where and how the necessary crypto keys, passwords, and other security secrets should be stored and distributed.*

Course 4

Course Title: *Management of Cybersecurity in the Cloud*
Corresponding Topic(s) from Coursera's Career Track Content List: (ignore if not creating Career Track content)
Course Project:

- **Title: Availability Plan**
- **Type: Peer Reviewed**
- **Prompt:** *For this project you will write a plan to cover likely risks to availability faced by an example cloud based application. Identify service providers responsible for each security measure in the plan. The application should provide high availability.*
- **Artifact:** *Through the project, learners will identify and select redundant data services to assure availability, and identify the types of service providers required.*

Course Learning Objectives: (3+ per course)

"In this course, a learner will be able to…"

- *Explain the process of vulnerability patching to minimize windows of vulnerability.*
- *Describe the elements of a secure cloud patching process, and how an effective process minimizes windows of vulnerability.*
- *Identify typical cloud availability risks (e.g. to data or services) and describe security techniques to address them.*
- *Describe key physical properties of a cloud provider's infrastructure that impact security of a cloud consumer's application.*
- *Discuss the role of auditing in the cloud management process: audit requirements, types of reports, impact of distributed architecture.*