RFP Final Project Template

Specialization Final Projects

This specialization contains four courses, each with its own project:

1. Basics of Cybersecurity in the Cloud
2. Data Security for the Cloud
3. Application Security for the Cloud
4. Administration of Cybersecurity in the Cloud

Final Project Overview #1

Course	*Basics of Cybersecurity in the Cloud*
Project Title	**Security Plan**
Project Prompt	*e.g., Learners will apply the business analytic skills to solve a real business problem company X is confronting now.* *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.*
Final Artifact	*Through the project, learners will learn to make a high-level risk assessment, design a basic security system to address the risks, and identify parties responsible for different cybersecurity roles.*
Assessment type for the final artifact submission	*Peer Review*

Peer Review Assignment Template #1

A peer review assignment, or peer-graded assignment, is an assignment in which learners review and grade each other's work. Peer review facilitates grading of open-ended assignments - such as essays, art, and design projects - in large online courses. Learn more about how peer review assignment works on Coursera here. More best practices of designing a good peer review assignment could be found here.

Assignment Overview	
Instructions and Learning Goals	*For this project, you will create a Security Plan for an example application implemented in the cloud using Platform as a Service. The plan should identify the security responsiblities of all service providers and indicate which security measures are provided by which providers.*
Grading Criteria	*The grade depends on the completeness of the answer in terms of covering material addressed in the course, including typical risks, security features of PaaS products, and security features required for business continuity.*
Assignment Time Estimate	*2 hours*
Prompt and Review Rubric (Provide at least one)	
Prompt #1	*List the risks faced by a cloud consumer who implements an application.*
Prompt #2	*Identify one or more typical security measures to address each risk.*
Prompt #3	*For each security measure, identify the service provider who must implement that measure.*
Prompt #4	*If a security measure is not provided by the cloud consumer, explain what assurance the provider gives to the consumer that the measure will be implemented effectively.*
Review Rubric	*#1: Does the list of risks contain at least one related primarily to confidentiality?* • Yes = 1 • No = 0 *#2: Does the list of risks contain at least one related primarily to integrity?* • Yes = 1 • No = 0

	#3: Does the list of risks contain at least one related primarily to availability? • Yes = 1 • No = 0 *#4: How complete is the list of risks considering the risks discussed in the course?* • Comprehensive = 4 • Not comprehensive but largely complete = 3 • Contains obvious gaps = 0 *#5: Is there at least one security measure associated with each risk? A measure may address more than one risk.* • *Yes = 5* • *Almost all of them = 4* • *Many of them = 3* • *Few of them = 2* • *The plan does not associate measures with risks = 0* *#6 Does each security measure identify the service provider responsible for it?* • *Yes = 5* • *Almost all of them = 4* • *Many of them = 3* • *Few of them = 2* • *The plan does not identify service providers = 0*

Final Project Overview #2

Course	*Data Security for the Cloud*
Project Title	**Data Distribution Plan**
Project 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.*

Final Artifact	*Through the project, learners will distribute data among cloud services to minimize the risk of spillage to unauthorized users.*
Assessment type for the final artifact submission	*Peer Review*

Peer Review Assignment Template #2

A peer review assignment, or peer-graded assignment, is an assignment in which learners review and grade each other's work. Peer review facilitates grading of open-ended assignments - such as essays, art, and design projects - in large online courses. Learn more about how peer review assignment works on Coursera here. More best practices of designing a good peer review assignment could be found here.

Assignment Overview	
Instructions and Learning Goals	*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.*
Grading Criteria	*The grade depends on the completeness of the answer in terms of covering material related to data classification, techniques to separate different actors from one another, and ways to connect to data from a database not authorized to actually handle the data.*
Assignment Time Estimate	*2 hours*
Prompt and Review Rubric (Provide at least one)	
Prompt #1	*Identify the different data classifications required by this application.*
Prompt #2	*Identify separate user roles required to provide "separation of duty" and "least privilege" in this application. Specify the type of access (read or write), if any, each role requires for each data classification.*

Prompt #3	*Distribute the data into separate databases to implement the separation of duty and least privilege. Identify each database and the types/classifications of data it contains.*
Prompt #4	*Associate the roles and access types described in Prompt #2 with each database in Prompt #3.*
Review Rubric	*#1: How many data classifications are identified?* • *3 or more = 3* • *2 = 2* • *1 or 0 = 0* *#2 Is there at least one separately identified role for each data classification, plus one for the end user?* • *Yes = 2* • *No = 0* *#3 Are there at least as many databases as there are data classifications?* • *Yes = 1* • *No = 0* *#4 Is every role associated with at least one database?* • *Yes = 2* • *No = 0* *#5 Is there any role that has read access to all databases?* • *Yes = 1* • *No = 0* *#6 Is there any role that has write access to more than one database?* • *Yes = 2* • *No = 0*

Final Project Overview #3

Course	*Application Security for the Cloud*
Project Title	**Key Management Plan**
Project 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.*
Final 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.*
Assessment type for the final artifact submission	*Peer Review*

Peer Review Assignment Template #3

A peer review assignment, or peer-graded assignment, is an assignment in which learners review and grade each other's work. Peer review facilitates grading of open-ended assignments - such as essays, art, and design projects - in large online courses. Learn more about how peer review assignment works on Coursera here. More best practices of designing a good peer review assignment could be found here.

Assignment Overview	
Instructions and Learning Goals	*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.*

Grading Criteria	*The grade depends on the completeness of the answer in terms of covering material addressed in the course, including typical cryptographic services used to secure an IaaS application, entities responsible for those services, and where keys would reside to support those services.*
Assignment Time Estimate	*2 hours*
Prompt and Review Rubric (Provide at least one)	
Prompt #1	*List the cryptographic services*
Prompt #2	*Identify one or more typical security measures to address each risk.*
Prompt #3	*For each security measure, identify the service provider who must implement that measure.*
Prompt #4	*If a security measure is not provided by the cloud consumer, explain what assurance the provider gives to the consumer that the measure will be implemented effectively.*
Review Rubric	*#1: Does the list of risks contain at least one related primarily to confidentiality?* • Yes = 1 • No = 0 *#2: Does the list of risks contain at least one related primarily to integrity?* • Yes = 1 • No = 0 *#3: Does the list of risks contain at least one related primarily to availability?* • Yes = 1 • No = 0 *#4: How complete is the list of risks considering the risks discussed in the course?* • Comprehensive = 4 • Not comprehensive but largely complete = 3 • Contains obvious gaps = 0 *#5: Is there at least one security measure associated with each risk? A measure may address more than one risk.* • *Yes = 5* • *Almost all of them = 4* • *Many of them = 3* • *Few of them = 2* • *The plan does not associate measures with risks = 0*

	#6 Does each security measure identify the service provider responsible for it? • *Yes = 5* • *Almost all of them = 4* • *Many of them = 3* • *Few of them = 2* • *The plan does not identify service providers = 0*

Final Project Overview #4

Course	*Administration of Cybersecurity in the Cloud*
Project Title	**Availability Plan**
Project 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.*
Final Artifact	*Through the project, learners will identify and select redundant data services to assure availability, and identify the types of service providers required.*
Assessment type for the final artifact submission	*Peer Review*

Peer Review Assignment Template #4

A peer review assignment, or peer-graded assignment, is an assignment in which learners review and grade each other's work. Peer review facilitates grading of open-ended assignments - such as essays, art, and design projects - in large online courses. Learn more about how peer review assignment works on Coursera here. More best practices of designing a good peer review assignment could be found here.

Assignment Overview	
Instructions and Learning Goals	*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.*
Grading Criteria	*The grade depends on the completeness of the answer in terms of covering material addressed in the course, including typical cryptographic services used to secure an IaaS application, entities responsible for those services, and where keys would reside to support those services.*
Assignment Time Estimate	*2 hours*
Prompt and Review Rubric (Provide at least one)	
Prompt #1	*List the cryptographic services*
Prompt #2	*Identify one or more typical security measures to address each risk.*
Prompt #3	*For each security measure, identify the service provider who must implement that measure.*
Prompt #4	*If a security measure is not provided by the cloud consumer, explain what assurance the provider gives to the consumer that the measure will be implemented effectively.*
Review Rubric	*#1: Does the list of risks contain at least one related primarily to confidentiality?* • Yes = 1 • No = 0 *#2: Does the list of risks contain at least one related primarily to integrity?* • Yes = 1 • No = 0 *#3: Does the list of risks contain at least one related primarily to availability?*

	• Yes = 1 • No = 0 *#4: How complete is the list of risks considering the risks discussed in the course?* • Comprehensive = 4 • Not comprehensive but largely complete = 3 • Contains obvious gaps = 0 *#5: Is there at least one security measure associated with each risk? A measure may address more than one risk.* • *Yes = 5* • *Almost all of them = 4* • *Many of them = 3* • *Few of them = 2* • *The plan does not associate measures with risks = 0* *#6 Does each security measure identify the service provider responsible for it?* • *Yes = 5* • *Almost all of them = 4* • *Many of them = 3* • *Few of them = 2* • *The plan does not identify service providers = 0*