## *Instructions*

*The Risk Management Project will be performed using the Clearwater IRM Analysis software. The software is cloud-based and may be accessed via a Web browser (Chrome or Firefox recommended). Each student will have an assigned account and will be provided access information prior to midterm.*

*Each phase is designed to take you through the exact same tasks an individual conducting a risk management program for an organization would perform, using the exact same tools that are currently available. The Clearwater software is currently the leading application for healthcare information risk management in the nation and as such you will find the software manual tailored for healthcare information systems.*

*Begin by reading through these instructions, and the associated detailed tutorial - available in D2L Content section. Review and/or complete the corresponding phase of this document before beginning the software component.*

*Clearwater Compliance, LLC Software (https://software.clearwatercompliance.com)*

***Be sure to place your personal information in this document header and delete everything in italics before submitting***

# PART 1 –INFORMATION ASSET INVENTORY AND RANKING

1. *Begin with the provided list of information assets the case organization would have and associate them with their media.*
2. *Complete Tables 1 and 2 in this document.*
3. *Add all information assets to Clearwater IRM Analysis Application (Under Asset Inventory)*
4. *Complete asset valuation screens in the Clearwater IRM Analysis application for your top information asset as defined in the template tables.*
5. *Ensure your asset descriptions are a minimum of 25 words in length.*
6. *Create component groups for all shared or dedicated components (media) associated with your information assets.*

***Then proceed to Part 2 as described in the CC|IRM tutorial (both are completed/uploaded together, as one submission).***

## TABLE 1 - LISTING OF INFORMATION ASSETS

*Instructions for Table 1. Delete before submitting.*

*Complete Table 1 below specifying any information assets appropriate to the case not provided (add/remove rows as needed), the component/media, owner, type of data, RTO, and RPO, of all provided information assets, based on assumptions you derive from the case document.*

*These values will be entered into CC|IRM later in the project. Remember, each application should be paired with its data on its own server. All data is backed to a NAS (External storage) daily, and all data and applications are backed to the cloud (Software-as-a-Service) weekly. Both NAS cross-backup daily as well (NAS 1 backs up to NAS 2 and vice versa). All employees access all information assets through their desktops.*

*Use the following options for the corresponding column’s values:*

### Component Group Options:

*Components (a.k.a. Media) are the devices that “create, receive, store, transmit or view” information assets. Essentially it’s the hardware that houses software and data. Before the current update for CC|IRM, these devices were referred to as media. For this project, use the following components:*

*Servers*

*External Storage (NAS1 and NAS2)*

*Desktops*

*Software-as-a-Service*

*Security and Governance*

*These component types are first entered when adding assets to CC|IRM, then you will reorganize these into groups that match the actual implementation in the case organization. For example: presume that the Human Resources Information Systems SERVER (Server A) contains a specialized HR application (referred to as HRIS), and a database of employee data. This application and its data are accessed by employees on DESKTOPS, with the database backed up to the EXTERNAL STORAGE (NAS1) on a daily basis, with both the HRIS and the database backed up to the SOFTWARE-AS-A-SERVICE (the cloud backup) on a weekly basis. Periodically, the organization’s InfoSec and Executive Management teams review the application and its database as part of their SECURITY AND GOVERNANCE duties. See where the Component Groups come into play with the two information assets (the HRIS and the Employee DB)? So under this example, the HRIS entries for Table 1 would be:*

| **Asset** | **Component/Media** | **Data Owner** | **Type of Sensitive Data** | **RTOTier** | **RPOTier** |
| --- | --- | --- | --- | --- | --- |
| 1. HRIS
 | DesktopServer (A)SaaS | HR Manager | PII | 3 | 3 |
| 1. HRIS (Employee) DB
 | DesktopServer (A)Disk Array (NAS1)SaaS | HR Manager | PII | 3 | 3 |

*(Note: I’ve just added numbers for the RTO and RPO. You should put some thought into the values for your project. If you just list them all the same or they don’t make sense, it could cost you points on the project).*

***Data Owner:*** *refer to the text for the definition of the data owner. While the CIO may be the data custodian, he/she is most likely NOT the owner of non-IT data.*

### Type of Sensitive Data Options:

* *Customer Confidential (Conf) – any data retained by the organization that has been labeled as confidential – i.e. limited in its access, distribution and use. Examples include executive meeting records; marketing and strategic plans not yet released; details of communications with and services provided to select client organizations; and company IT and InfoSec program details.*
* *Electronic Patient Healthcare Information (ePHI) – any data retained by the organization that contains personal medical information, including that of employees and clients. Employee health coverage information in an HR file is not ePHI for our purposes – unless it included details on the coverage such as the account number, primary care physician, etc. Most HR records would only contain the name of the coverage (e.g. Blue Cross/Blue Shield HMO), but not the details.*
* *Payment Card Information (PCI) – any data retained by the organization that contains payment card information such as debit/credit card numbers with expiration dates, users’ names, security codes and/or billing information.*
* *Personally Identifiable Information (PII) – any data retained by the organization that contains personally identifiable information that could be used to identify an individual (or steal their identity) including names with social security numbers, driver’s license numbers, addresses, phone numbers, family members.*
* *Student Records (FERPA) – any data retained by the organization that contains academic information regarding an individual including names with student numbers, social security numbers, courses taken, grades assigned, academic integrity/misconduct issues, financial aid and/or other PII.*

 *For our purposes, ePHI and FERPA are considered specialized versions of PII. If a data asset has no academic or medical content, just classify it as PII. If a component group contains multiple different classified data assets, list all that it contains.*

### RTO Tiers Options:

*“Recovery time objective (RTO) is the maximum desired length of time allowed between an unexpected failure or disaster and the resumption of normal operations and service levels. The RTO defines the point in time after a failure or disaster at which the consequences of the interruption become unacceptable.” (CC|IRM Help Menu). Refer to the text pp. 509-10 for additional discussion of this topic.*

*0 = less than 1 hour*

*1 = 1 – 2 hours*

*2 = 3 – 6 hours*

*3= 6 – 24 hours*

*4= 1 – 3 days*

*5= 3 – 5 days*

### RPO Tiers Options:

*“A recovery point objective (RPO) is the maximum acceptable amount of data loss measured in time. It is the age of the files or data in backup storage required to resume normal operations if a computer system or network failure occurs.” (CC|IRM Help Menu). Refer to the text pp. 509-10 for additional discussion of this topic.*

*0 = less than 1 hour*

*1 = 1 – 2 hours*

*2 = 3 – 6 hours*

*3= 6 – 24 hours*

*4= 1 – 3 days*

*5= 3 – 5 days*

*A few Assets have been added to the table to help you get started. You will need to identify the rest on your own. Add rows as needed.*

**Table 1: Listing of Information Assets for *Case Organization***

| **Asset** | **Component/Media** | **Data Owner** | **Type of Sensitive Data** | **RTO** | **RPO** |
| --- | --- | --- | --- | --- | --- |
| 1. AD Service
 | DesktopServer ASaaS | CIO |  |  |  |
| 1. AD SQL DB
 | DesktopServer ANAS1SaaS | CIO |  |  |  |
| 1. DNS Service
 | DesktopServer ASaaS | CIO |  |  |  |
| 1. DNS SQL DB
 | DesktopServer ANAS1SaaS | CIO |  |  |  |
| 1. Exchange email app.
 |  |  |  |  |  |
| 1. Email DB
 |  |  |  |  |  |
| 1. NAS1 App.
 |  |  |  |  |  |
| 1. NAS1 Data
 |  |  |  |  |  |
| 1. NAS2 App.
 |  |  |  |  |  |
| 1. NAS2 Data
 |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

## TABLE 2 – WEIGHTED RANKING OF INFORMATION ASSETS

*Instructions for Table 2. Delete before submitting.*

*Create a weighted table analysis, as described in the text, to rank all information assets from Table 1. To assist you in the calculations, you may use the Weighted Ranking of Information Assets spreadsheet provided in D2L.*

1. *Identify 4-5 criteria you will use to evaluate the assets identified earlier, and assign weights to the criteria. Note the weights must sum to 1.0 (as in 100%).*
2. *Copy the complete list of assets from Table 1 into the first column of Table 2.*
3. *Evaluate each information asset against your criteria by assigning a value of 0 to 5 (with 5 being most critical) under each asset criterion. Use the following scale in your assignments, to answer the question: “How important is this asset with regard to this criterion?”*
	1. *5 - Critically important*
	2. *4 - Very important*
	3. *3 - Important*
	4. *2 - Somewhat important*
	5. *1 - A little important*
	6. *0 - Not important*
4. *Perform the calculations to determine the totals. (each cell is multiplied by its criterion’s weight, then all products are summed into the total column).
Note: sample criteria weights were added to the table to illustrate function (e.g. Crit 1; .20). Replace these values with your own criteria and weights.*
5. *Use the following scale to convert the weighted table analysis “Total” values to Clearwater “Importance” scores. Use standard rounding (e.g. .5 and above rounded up) to select the corresponding Importance score:*
	1. *5 - Critically important*
	2. *4 - Very important*
	3. *3 - Important*
	4. *2 - Somewhat important*
	5. *1 - A little important*
	6. *0 - Not important*

*Row 1 provides an example of a completed row. Replace this row’s values with your own before submitting.*

1. *Finally sort the entire table on the Total column. When you’re finished, your number one asset (first on the list) should be the one with the largest total, and thus the highest importance.

Refer to the supplemental lecture on Weighted tables for additional instructions.*

**Table 2: Weighted Ranking of Information Assets**

| **Criteria 🡺** | ***InsertCrit 1******here*** | ***InsertCrit 2******here*** | ***InsertCrit 3******here*** | ***InsertCrit 4******here*** | ***InsertCrit 5******here*** | **Total*****0-5.0*** | **Importance*****(0-5; Not Important to Critically Important)*** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Criteria Weight🡺****🡻Asset Name** | ***Insert Crit 1 weight******here*** | ***Insert Crit 2 weight******here*** | ***Insert Crit 3 weight******here*** | ***Insert Crit 4 weight******here*** | ***Insert Crit 5 weight******here*** |  |  |
| 1. AD/DNS Services
 | *3* | *3* | *4* | *2* | *3* | *3.00* | *3 – Important* |
| 1. DNS DB
 |  |  |  |  |  |  |  |
| 1. AD SQL DB
 |  |  |  |  |  |  |  |
| 1. Exchange email app.
 |  |  |  |  |  |  |  |
| 1. Email DB
 |  |  |  |  |  |  |  |
| 1. NAS1 app.
 |  |  |  |  |  |  |  |
| 1. NAS1 Data
 |  |  |  |  |  |  |  |
| 1. NAS2 app.
 |  |  |  |  |  |  |  |
| 1. NAS2 Data
 |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

**Criteria Descriptions:** *List and describe your criteria used in Table 2 below. Then provide a detailed justification as to how and why you selected these criteria and their weights.*

*Format: Criterion (e.g. Impact on Profitability) – this criterion is defined as \_\_\_\_\_, This criterion was selected because \_\_\_\_\_, A weight of \_\_\_ was selected for this criterion because \_\_\_\_\_.*1.

2.

3.

4.

5.

## PART 2: RISK DETERMINATION & RISK RESPONSE

 *At this point you should download and follow the instructions on the RM Project tutorial, which will take you through the Clearwater Compliance | IRM portion of the assignment. The steps to be performed and deliverables for the overall assignment are listed in that document. This document, plus the Reports you will generate at the end of the tutorial are your deliverables for the RM assignment. However, I will be accessing your CC|IRM account directly to do much of the grading. Remember to delete all instructions in italics before submitting this document.*

*The application uses a slightly different definition of risk treatments (we call them risk controls): Use their definitions for the application, but the text’s for all assignments.*

*“Risk acceptance is the appropriate risk response when the identified risk is within the organizational risk tolerance. Organizations can accept risk deemed to be low, moderate, or high depending on particular situations or conditions.” (In the Text we also label this as Acceptance)*

*“Risk avoidance may be the appropriate risk response when the identified risk exceeds the organizational risk tolerance. Organizations may conduct certain types of activities or employ certain types of information technologies that result in risk that is unacceptable. In such situations, risk avoidance involves taking specific actions to eliminate the activities or technologies that are the basis for the risk or to revise or reposition these activities or technologies in the organizational mission/business processes to avoid the potential for unacceptable risk.” (In the Text we label this as Termination)*

*“Risk mitigation, or risk reduction, is the appropriate risk response for that portion of risk that cannot be accepted, avoided, shared, or transferred.” It typically involves the implementation of new or enhanced controls and counter-measures. In the Text we label this as Defense)*

*“Risk sharing or risk transfer is the appropriate risk response when organizations desire and have the means to shift risk liability and responsibility to other organizations.” (In the Text we label this as Transfer)*

*In some case more than one Risk Treatment might be an appropriate response to a risk. It is common for Transfer and Mitigation activities to both be applied to reduce a risk. Select a primary risk treatment type and select or add controls or recommendations that correspond to all Risk Treatment types in the Evaluate Alternatives section.*

*If you select “Mitigate” (most common), then specify expected Effectiveness of proposed controls, estimated cost, feasibility and whether the action will enhance (improve) or add (new) the control, or if that control is effective (no change), or needs to be removed (omit).*