Risk Assessment Exercise Breakout #3 (WORKSHEET) – Scoring

Scoring

	Methodology Steps	*Project-Specific Details*
	Choose Scale: It is important to define a consistent scale for: • **Asset Importance** – How important is the asset relative to other assets? Do not hesitate to document assets that are of low importance, they will be addressed when we prioritize & trim. • **Risk Impact** – What is the potential impact of the raw, unmitigated, inherent risk? • **Risk Likelihood** – What is the potential likelihood of the raw, unmitigated, inherent risk? • **Control Design** – How effective is the design of the control against most associated risks? • **Control Execution** – How effective have you implemented the control at this particular institution?	*How would you rate your assets?* *What is the level of potential impact if a risk affected Bank assets?* *What is the likelihood that a risk will have an impact on Bank assets?* *How well designed is this control to mitigate risk? Can it effectively mitigate a risk?* *How well executed in your environment is this control? Are you consistently performing a control?* *Can you defend whatever scale you choose and why did you select that scale? Can you defend your control execution?*
	Identify Inherent Risk?	*How did you identify which risks were inherently more risky than others?* _____ _____ *Remember Raw Inherent Risk assumes that no controls are applied. Difficult concept since we typically want to apply controls when thinking about it. Especially when setting Likelihood!!* *Any Risk that rates "H" should be audited on what frequency* _____*?* *Any Risk that rates "L" or "M" should be audited how often* _____*?* *Do you create a 3-4 Year Audit and Risk Management Plan?*

LIKELIHOOD	IMPACT				
	Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Catastrophic (5)
(5) High	M	M	H	H	H
(4) Likely	M	M	M	H	H
(3) Maybe	L	M	M	H	H
(2) Could	L	L	M	M	M
(1) Rare	L	L	M	M	M

Scoring		
	Methodology Steps	***Project-Specific Details***
	Choose Reporting Scale: A tool may provide an ability to do fancy mapping and calculations. Map your Mitigation % (Residual Risk) to Mitigation Level (H-L). Consider how you establish your scoring matrix, and what can be done using an institution and/or assessment-specific cutoff based on the asset importance.	*During this step of the assessment, what kinds of discussion could you have about risk? Is residual risk of Medium adequate for a medium importance asset? Low for a Medium?* *Any Important Asset with a Low Mitigation (1 or L) is considered poorly protected.*

Asset Universe Scoring		
	Asset Importance Scoring and Normalizing: ▪ First-pass: Score each asset independently. ▪ Second-pass: Normalize the scores by reviewing all universe items with respect to each other. This is meant to be a sanity-check to confirm consistent and reasonable scoring. This is usually easier if one team scored all items. Otherwise, the normalization step will identify risk assessment teams who were inconsistent; scoring things higher or lower than other areas.	*Assign Scoring to Assets. Importance based on value, criticality and confidentiality of data.* *Consider the Assets characteristics/attributes from the Universe Definition Process.*
	Asset Universe: Prioritize and Trim. Remove or make note of Low-Importance Assets that can be ignored in the scope of the rest of the risk assessment process.	*Review any low importance assets compared to high importance, are there any? Eliminate areas that your institution may not offer; Cash Management, Mobile Banking, RDC.*
	Asset Universe Scoring: Are there any potential observations/findings from the process of identifying assets? • Sort by Importance. • Filter by Attributes. For example, consider all assets that process, transmit or store non-public personal customer information. Can features/data be manipulated both internal and externally by the customer? • This step is exploratory in nature. Spend some time and look for trends.	*Validate the potential high importance assets, considering risks and controls that were noted after association was performed to determine potential control deficiencies, or missing risks.*

Risk Universe Scoring		
	Risk Impact and Likelihood Scoring and Normalizing: ▪ First-pass: Score each item independently. ▪ Second-pass: Normalize the scores by reviewing all universe items with respect to each other. This is meant to be a sanity-check to confirm consistent and reasonable scoring. This is usually easier if one team scored all items. Otherwise, the normalization step may identify where risk assessment teams were inconsistent with the scoring, some set things higher or lower than other areas.	*Assign the inherent Risk Impact and Risk Likelihood on a scale of 1-5 while considering the Risk Characterization and other factors.* *Will one team, sub-groups or only a single person be performing the scoring and will you have full-group reviews.*

	Risk Universe: Prioritize and Trim. Remove or make note of low-impact or low-likelihood risks that can be ignored in the scope of the rest of the risk assessment process.	*We reviewed the risks areas with low inherent risk.* *Generally, this was used as a trimming step to identify out-of-scope risk areas. These were archived from the system to keep the risk universe clean and relevant to our institution.*
	Risk Universe Scoring: Are there any potential observations/findings from the process of identifying assets? • Sort by Impact and Likelihood. • Filter by Attributes. For example, do a query for all risks related to "Technology Changes" as a basis for project-specific risk assessments. • This step is exploratory in nature. Spend some time and look for trends.	*Several potential high risk areas were identified.* _____ *These were noted after association was performed to see the final applied control deficiencies.*
	Risk Universe Scoring: Identify Future Areas	*It is helpful to know how to query the database for future risk assessments. For example, if we are considering adoption of new technology, the risk universe can help us identify potential risk areas.*
	Risk Universe Scoring: Exceptional Areas.	*Do we stand out in some way?*

Control Universe Scoring		
	Control Design and Execution Scoring and Normalizing: ▪ First-pass: Score each item independently. ▪ Second-pass: Normalize the scores by reviewing all universe items with respect to each other. This is meant to be a sanity-check to confirm consistent and reasonable scoring. This is usually easier if one team scored all items. Otherwise, the normalization step will identify risk assessment teams who were inconsistent with the scoring things higher or lower than other areas.	*We carefully scored the Control Design and Control Execution on a scale of 1-5 while considering the Control Characterization Attributes and other factors.* *The Source documents were critical in this process.* *It was one team performing the scoring with individual, sub-group and full-group reviews.* *The normalized result was a reasonable and appropriate mix of scores.*
	Control Universe: Prioritize and Trim. Usually there is nothing to do here from a scoring perspective. From a normalization perspective, you may choose to remove redundant control items from the universe.	*We reviewed the control areas trying to identify redundant items.* *These were archived from the system to keep the control*

		universe clean and relevant to our institution.
	Control Universe Scoring: Are there any potential observations/findings from the process of identifying assets? • Sort by Execution. This is a typical way to identify control deficiencies. • Filter by Attributes. • This step is exploratory in nature. Spend some time and look for trends.	*Several potential control deficiencies were identified.* _____ *These were noted until after association was performed to see the final applied control deficiencies.*
	Control Universe Scoring: Identify Future Areas	*It is helpful to know how to query the database for future risk assessments. For example, we considered future plans for control implementation and found that there was a scheduled project related to _____ that may not provide the best return on investment.*
	Control Universe Scoring: Exceptional Areas.	*We discussed some areas of obvious strength. For example, the _____is a very strong control for an institution of our size and complexity.*
Association – Assets to Risks		
	Asset-Risk Association: • For each Asset, assign the most relevant risk areas. The idea is to cover the risk universe, not to overstate the obvious. (For example, you could relate the risk of "Natural Disaster" with every Asset. A more common-sense approach is to relate it to the physical assets, such as data centers and people with an implied or documented dependency to other assets such as individual servers or applications. • For each Risk, assign the most relevant Assets. This is a cross-check to make sure that Asset-Risk association covers the asset universe.	*Step through the Risk and the Risk-Asset steps to provide reasonable coverage of the most relevant relationships.*
	Asset-Risk Inherent Risk Detail Review: • For each asset, examine the Risk Impact and Risk Likelihood scores. While most follow the defaults, look for anomalies.	*Review the Risk Impact and Likelihoods to see if there was anything that didn't make sense.*

	Asset-Risk Association: Are there potential observations/findings related to Asset-Risk Association? • Are there Assets with insufficient risks? • Are there Risks that have not been applied appropriately to Assets?	*Did anything unusual come up in this process?*
	Asset-Risk Association: Identify Future Areas	*There is always room for more refinement. Establish a manageable set of relationships that can be expanded in the future.*
	Asset-Risk Association Scoring: Exceptional Areas.	*Do we stand out in some way?*
Association – Risks to Controls		
	Risk-Control Association: • For each Risk, assign the most relevant Control areas. The idea is to cover the risk universe, not to overstate the obvious. • For each Control, assign the most relevant Risks. This is a cross-check to make sure that Risk-Control association provides appropriate coverage.	1. *We started with the associations already identified in* _____. 2. *We combined the list with the standard associations from RiskOptix®.* 3. *We stepped through the Risk-Control and the Control-Risk steps to provide reasonable coverage of the most relevant relationships. Ultimately, this is covered on the Audit | Assessment Asset-Risk-Control Detailed Assessment.*
	Risk-Control Unapplied Residual Risk Detail Review: • For each Risk and Controls, review the Impact, Likelihood, Design and Execution.	*Make adjustments as necessary here.*
	Risk-Control Association: Are the potential observations/findings related to Risk-Control Association? • Are there Risks with insufficient Controls? • Are there Controls that have not been applied appropriately to Risks?	*Can you recognize Control Deficiencies? Controls not implemented that should be for an Asset – Risk paring or that are not consistently being followed in our institution (poor implementation).*
	Risk-Control Association: Identify Future Areas	*There is always room for more refinement. Our approach was to maintain a manageable set of relationships that can be expanded in the future.*
	Risk-Control Association Scoring: Exceptional Areas.	*Do we stand out in some way?*
Association – Assets, Risks and Controls (ARC)		
	ARC Review: Review the Asset-Risk-Control (ARC) in the project scope to identify: 1. Risks which have a different Impact/Likelihood against particular assets. 2. Controls which have a different Design/Execution against particular Risks or particular Asset-Risk pairs. 3. Controls which are Not Applicable (N/A) to a particular Asset-Risk Pair.	*Step through the ARC summary; discuss whether you feel you have a reasonable coverage of the most relevant relationships.* *In a bigger assessment you may review the Asset-Risk-Control Detailed list with an emphasis only on the more important assets and the most likely areas of control deficiencies.*

	ARC: Are the potential observations/findings? • Are there Asset-Risk Pairs with insufficient Controls? • Are there Assets with unacceptable mitigation levels? • This is an exploratory step.	*Further identify any control deficiencies by comparing the ARC Details by Control Execution.* *Are there controls that you feel may not have a significant impact on the risk posture of the institution?*
	ARC: Identify Future Areas	*There is always room for more refinement.* *Can you identify control deficiencies for significant areas of improvement? Future risk assessments may spend more time examining control efficiency. In any case, it is imperative to "use your brain" to look for practical responses. (Common Sense)*
	ARC: Exceptional Areas.	*What are you doing right?*