Risk Assessment Exercise Breakout #3 (ANSWER SHEET) – Scoring

Scoring		
	Methodology Steps	***Project-Specific Details***

	Choose Input 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 appropriately whey we prioritize & trim in a later step.
	• **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?
	  ○ For example, even the most effective "Acceptable Use Policy" would still only have limited effectiveness against the risk of Employee Fraud.
	  ○ Another example, Anti-Virus software; by design, it is thought to be quite effective at reducing the risk of the outbreak of malicious code.
	• **Control Execution** – How effective is the execution or implementation of the control at your institution?
	  ○ For example, is there an "Acceptable Use Policy?" Is it reviewed on a regular basis? Is it enforced?
	  ○ Another example is if all desktop machines have Anti-Virus software installed? Do you have centralized management capabilities to prove it?
		What Scale did you use for rating the Risk Universe?
		
		We choose to use a consistent scale from 1 to 5, with 5 being the "greatest - high" 1 being "smallest – low".
		
		Examples:
		• Asset Importance of 1 – lowest importance asset classification.
		• Risk Impact/Likelihood of 5 – highest inherent risk.
		• For a Control Execution of 2 – the control may exist, but there are known deficiencies.
		
		Where appropriate, the scoring 1-5 may consider financial, strategic, reputation and other risk categories.
		
		During the first pass of discussion we simply used low, medium, and high or numerically 1, 3, and 5. The scores of 2 and 4 were used to make finer distinctions or break ties, differentiate between two areas.
		
		The most important steps are the ***process*** used to identify the scores (the discussion) with appropriate notes added to the risk assessment for reporting situations, concerns, and reasons to explain and justify any score.

Identify Inherent Risk?

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

How did you identify which risks were inherently more risky than others?

- If a risk is highly (5) likely to occur and has a high impact (5) the inherent risk is subsequently high (5)
- If it has a low likelihood (1) and low impact (1) inherent risk is subsequently low.

Remember Raw Inherent Risk assumes that no controls are applied. Difficult concept sometimes as we all want to apply controls when setting it.

Any Risk that rates "H" should be audited on what frequency (POLICY driven) _____?

Any Risk that rates "L" or "M" should be audited how often _____?

From an inherent risk perspective, our process showed likely areas to audit more frequently.

Choose Output Scale:
Your Tool may automatically compute the following types of values:

- **Mitigation %** - Were you able to determine how well mitigated you are against specific risks based on how well implemented your controls are?

  For Example: Can you create a summary of the strength of controls with respect to the applied combinations of asset-risk pairs.
  Here is a simple example:
  - Asset "A" has only one risk associated with it. The risk has an Impact of 5 and a Likelihood of 5. The asset-risk pair has only one control which has a Design Score of 4 and an Execution Score of 4. In this example, the Mitigation % would be AVG (4/5, 4/5) which is 4/5 or 80%.
- **Residual %** - A summary of the unmitigated risk due to the strength of controls with respect to the applied asset-risk pairs. It is the inverse of how well mitigated you feel you are 100% - calculated Mitigation %.
  In the above example, it would be 100%-80% leaving 20% Residual

Reviewed the results of the scoring in our tool.

Mitigation % (Residual Risk) provides a deeper level of insight than a simple scale of 1-5 while considering the relative number and strength of applied controls.

You can calculate how well protected an asset may be based on a specific control.

A simplistic risk assessment output scale might simply report on how well an asset is protected using the 1-5 (L,ML M,MH, H) or some other scale,

	Risk. Note: 99% is the highest allowed Mitigation%, since nothing is ever 100% mitigated even if every applied control is a Design and Execution of 5, there always remains a potential impact and likelihood something bad will happen.	even 3-1 (L,M,H), Low to High (0% - 99%), or ?. Typically even if a fancy scale is used it will all boil down to High, Medium or Low Risk when reporting to management. Much of Residual risk is a gut feeling as much as you'd like it to be scientific.
	Choose Reporting Scale: A tool may provide an ability to map your Mitigation % to Mitigation Level (H-L). You can establish your scoring matrix, and can be done using institution and/or assessment-specific cutoffs based on the asset importance.  5 = very important asset – must be mitigated to at least 80% to receive a 5 mitigation level or "High". 1 = insignificant asset only need to be mitigated at 50%	*During this step of the assessment, you can show whether there is significant Asset residual risk exposure by sorting by your Mitigation Level.* *Any Important Asset with a Low Mitigation (1 or L) is considered poorly protected.* <u>Can do "What If" discussion; from an residual risk perspective, our scoring showed we have important assets where we can improve controls. What if we buy, what if we implement, what if we ask management?</u>

Asset Universe Scoring		
	Asset Importance 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. Often the challenge when an IT Risk Assessment is done with one spreadsheet and the BSA or another risk assessment is done with another. The methodology and scoring is not consistent. Importance of a server might be high in one and low in another. The server remains consistent in its importance; it's the value of that server in relationship to the assessment being done. For example it has no BSA data associated with it.	We carefully scored the Asset Importance on a scale of 1-5 while considering the Asset Characterization and other factors. Discuss as a cross functional team (**process**) to perform the scoring – you may consider individual, sub-group and full-group reviews to ask questions and force the team to justify the scoring. The normalized result was a reasonable and appropriate mix of low, medium and high importance scores.

	Asset Universe: Prioritize and Trim. Remove or make note of Low-Importance Assets and decide how they will be handed; can they be ignored in the scope of the rest of the risk assessment process.	We reviewed the low importance assets. Can we ignore them? *Are there assets to keep in the universe since they may be something that is implemented in the future?*
	Asset Universe Scoring: Are there any potential observations/findings from the process of identifying assets? • Sort by Importance. • Filter by Attributes. For example, do a query for all assets that process, transmit or store non-public personal customer information. • This step is exploratory in nature. Spend some time and look for trends.	*Several potential high importance assets were identified. _____.* *These were noted after association was performed to see the final applied control deficiencies.*
	Asset Universe Scoring: Identify Future Areas	*Refinement of the Mitigation Level Thresholds is a good item to consider for future refinement. Increase Mitigation percent with control maturity. (80% to 85%)*
	Asset Universe Scoring: Exceptional Areas.	Nothing noted.

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 will identify risk assessment teams who were inconsistent with the scoring things higher or lower than other areas.	We carefully scored the inherent Risk Impact and Risk Likelihood on a scale of 1-5 while considering the Risk Characterization and other factors. Discuss as a cross functional team to perform the scoring; you may consider individual, sub-group and full-group reviews to ask questions and force the team to justify the scoring. <u>The normalized result was a reasonable and appropriate mix of scores.</u>
	Risk Universe: Prioritize and Trim. Remove or make note of low-impact or low-likelihood risks. Consider whether they can be ignored in the scope of the rest of the risk assessment process.	We reviewed any risks areas with low inherent risk. Use as a trimming step to identify out-of-scope risk areas. Or areas where we don't need to focus. Do you apply more controls to low risk? Notlikely!

	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 a project-specific risk assessment. • This step is exploratory in nature. Spend some time and look for trends.	Potential high risk areas were identified. External Fraud, Account Takeover, Customer Error and Omissions. These were noted after association was performed to see the final applied control deficiencies. Example: No customer education program.
	Risk Universe Scoring: Identify Future Areas	It is helpful to know how to use the information you've gathered for future risk assessments. For example, if we are considering adoption of a new technology, the risk universe can help us identify potential risk areas and controls where improvements may be necessary. Think Mobile Banking, make customer more aware of protecting their phone with passwords to protect account access if it were lost. Analysis of the risks may determine this new product require other control purchases or upgrades before implementation. Online Banking Cash Management = need a solution to detect fraud and prevent account takeover.
	Risk Universe Scoring: Exceptional Areas.	*Nothing noted.*

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 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.* Discuss as a cross functional team to perform the scoring;

		you may consider individual, sub-group and full-group reviews to ask questions and force the team to justify the scoring.
	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.* Termination Procedures or Access Control Procedures *These were archived from the system to keep the control universe clean and relevant to our institution. Example: At a later date it may be determined termination procedures are more important and need focus for some reason.*
	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.	Identify potential control deficiencies. Ex: Access Controls poorly implemented. These were noted until after association was performed to see the final applied control deficiencies.
	Control Universe Scoring: Identify Future Areas	Consider and document future plans for control implementation. Ex: Identified that there was a scheduled project related to new software for customers called eBankSafe to prevent Customer Account takeover and provide customer education/awareness.
	Control Universe Scoring: Exceptional Areas.	*We discussed some areas of obvious strength. For example, our - Ex:* • *Fraud detection reporting* • *Customer Education* • *Access Controls* • *Software supplied to customers* *were very strong control for an institution of our size and complexity.*

Association – Assets to Risks (linking your 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.	1. We started with the associations already identified from our inventory. 2. We combined the list with the standard associations from our tool. *3.* We stepped through the Asset-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.	We reviewed the Risk Impact and Likelihoods to see if there was anything that didn't make sense. Adjustments were made as felt needed.
	Asset-Risk Association: Are the 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?	You may spend significant time as individuals, sub-groups and as a group reviewing the associations until you feel they are appropriate for the size and complexity of the institution.
	Asset-Risk Association: Identify Future Areas	There may always be room for more refinement. Our approach was to maintain a manageable set of relationships that can be expanded in the future. Don't get caught in analysis-paralysis.
	Asset-Risk Association Scoring: Exceptional Areas.	*Nothing noted.*

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 from our inventory, and past risk assessment. 2. We combined the list with the standard associations from our Tool®. *3.* We stepped through the Risk-Control and the Control-Risk steps to provide reasonable coverage of the most relevant relationships.
	Risk-Control Unapplied Residual Risk Detail Review: • For each Risk and Controls, review the Risk Impact-Likelihood and Control Design-Execution.	*Several adjustments may be made.*

	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?	We spent some time as individuals and sub-groups reviewing the associations. We feel they are appropriate for the size and complexity of the institution. Or we made changes felt necessary.
	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.	*Nothing noted.*
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 relationships to ensure reasonable coverage of the most relevant relationships. Consider emphasis on the more important assets and the most likely areas of control deficiencies. Several adjustments may be made.
	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.	*Were control deficiencies identified by review of the ARC Details by Control Execution?* Look for poorly implemented controls for deficiencies. Risks that don't have a direct impact or area overly broadly applied. Verify control assignment.
	ARC: Identify Future Areas	There is always room for more refinement. *For this risk assessment, there were sufficient control deficiencies identified to provide significant areas of improvement. Future risk assessments may spend more time examining control efficiency.* In any case, it is imperative to "use your brain" and common sense to look for practical responses. Tools can assist in answering questions about the scoring. If you don't have some discussion in this area you may end up implementing controls that are too specific or not cost effective for the risk mitigated.
	ARC: Exceptional Areas.	*Nothing noted.*