











Risk Assessment Breakout #1 Exercise (ANSWER SHEET) – Preparation

Preparation		
	Methodology Steps	Project-Specific Details
	<p>Define Purpose, Scope, Goals:</p> <ul style="list-style-type: none"> Which business areas will be covered? What context applies? Is this a risk assessment, audit or review? 	<p><i>The purpose of the project is to perform a</i></p> <ul style="list-style-type: none"> Online Banking Risk Assessment? Controls Risk Assessment? Business Continuity Risk Assessment? Enterprise-wide Information Technology Risk Assessment BSA Risk Assessment <p>The assessment will address the administrative, technical, and physical safeguards for a bank of our size and complexity.</p> <p>The scope of the risk assessment process needs to ensure that all reasonable foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information are considered.</p> <p>The goal will be to assess the probability or impact of inherent risk while also calculating residual risk based on the effectiveness of the perceived design and execution of controls.</p>
	<p>Identify the Specific Purpose:</p> <ul style="list-style-type: none"> Audit Planning Budgeting Compliance Disaster Recovery Policy Writing Risk Management Remediation Vendor Selection 	<p><i>During the preparation phase we identify the approach and the purpose of the risk assessment.</i></p> <p><i>The specific purpose for this assessment was to:</i></p> <ol style="list-style-type: none"> Provide assistance in determining which future projects to perform so as to ensure that areas of highest risk are given a higher prioritization over projects than those with a lower level of risk. Establish a sustainable risk assessment methodology that allows the bank to continuously monitor the level of risk. Increase compliance with federal regulations related to the safeguarding of customer information – specific to Online Banking Authentication Guidance.
	<p>Anticipate the Benefits:</p> <ul style="list-style-type: none"> To learn something new To validate or quantify a concern To standardize communication of risk To establish common language and 	<p><i>The anticipated benefits for this engagement:</i></p> <ul style="list-style-type: none"> To establish common language and tools To establish a way to link Risk Assessment to project prioritization. To standardize communication of risk.

Preparation		
	Methodology Steps	Project-Specific Details
	tools <ul style="list-style-type: none"> To satisfy regulatory requirements 	<ul style="list-style-type: none"> To improve on existing risk assessment processes. Meet regulatory requirement of Authentication Guidance by providing an Online Banking Risk Assessment.
	Decide to In-source or Outsource: <ul style="list-style-type: none"> Confirm that you have the capability in-house. Engage an external firm with independent, knowledgeable and sufficient resources. 	Did you need to engagement with an external consulting firm to help provide risk assessment expertise?
	Evaluate Automation Options: <ul style="list-style-type: none"> Paper Excel / Word Specialized Software 	Risk Assessment software was used for the risk assessment. (RiskOptix®) Risk Assessment software was not used for the risk assessment. (spreadsheets, word)
	Identify Source Documents: <ul style="list-style-type: none"> Strategic Plans – is the business changing? List of Related Projects (Recent and Planned). Prior Audits/Examinations. New guidance about threats. 	<i>Here is the list of the most significant source documents for the risk assessment.</i> <ul style="list-style-type: none"> Information Security Program Information Security Policy Manual ?
	Earn Management Buy-In: <ul style="list-style-type: none"> Identify Motivators Assign Project Sponsor Approve Resources 	There is full management buy-in that this is an important strategic and tactical step. Not simply because of compliance, but to help focus and improve the information security posture of the institution. <i>Project Sponsor: Who? (IT, Compliance, Internal Audit, Operations Officer, President/CEO.)</i> <i>Resources Approved: Internal resources, external consultants and an automated tool.</i>
	Preparation Stage Review: <ul style="list-style-type: none"> Are all steps addressed? Are there any areas that are excluded? 	The preparation stage was completed with no questions about the proper completion of each step.
	Preparation Stage Potential Observations/Findings: <ul style="list-style-type: none"> Are there any potential areas of concern? The purpose is to make notes. A big concern at this stage may not be an issue in the context of the completed risk assessment. Nonetheless, it is important to document suspected areas of improvement. 	The scope is much more involved than what was performed in the past. We may implement mobile banking, should we assess it now? When to assess new products? There is a concern about finding a balance that matches the size and complexity of the institution.
	Preparation Stage Potential Areas of Excellence: <ul style="list-style-type: none"> Are there noteworthy areas of excellence? 	None identified in the Preparation Stage.