# Risk Assessment Breakout #2 Exercise (ANSWER SHEET) – Universe Definition

| Universe Definition | |
|---|---|
| **Methodology Steps** | ***Project-Specific Details*** |
| Define the approach.<br>• "Assets", "Risks" and "Controls"<br>• Granularity<br>• Level of Detail | The approach will be to assess the Assets, Risks and Controls related to online banking.<br><br>For level of granularity we could select key functions to recognize; bill pay, cash management, online loan applications, electronic check ordering, eStatements.<br><br>The level of detail we did not choose to identify specific customers, or features within a function, i.e. specific places where the customer does bill pay, check ordering vendors or other banks where they receive payroll deposits from. We didn't worry about each piece of back office software that might be used; excel, word, etc.. |

| Universe Definition – Assets | |
|---|---|
| **Methodology Steps** | |
| Asset Universe Granularity.<br>• How many levels of assets do we want to consider?<br>• Where will the asset list come from?<br>• What process will be used to determine the level that is appropriate for the size and complexity of the institution? | 1. *We started with the list of Assets from:* EXPERIENCE.<br>2. We combined the list with the assets provided from our tool's library.<br>3. We reviewed the source documents (software list, vendor list) to ensure appropriate coverage.<br>4. The process carefully considered appropriateness for the size and complexity of the institution while considering the Scope and Specific Purpose of this particular assessment. |
| Asset Universe Level of Detail.<br>How much information do we want to understand for each asset? This is known as "characterizing" assets.<br><br>Here is a conceptual example of a simple approach to characterization. Select a set of attributes that are appropriate for the size and complexity of the institution while supporting the risk assessment project scope and specific purpose. | 1. We started with attributes we discussed as a team.<br>2. We combined the list with the standard attributes from our tool.<br>3. We disabled any attributes that did not apply to the scope of the project.<br>4. We added additional attributes as appropriate into the database which allow us to filter and sort based on the asset characterization. |

| Universe Definition | |
|---|---|
| **Methodology Steps** | ***Project-Specific Details*** |
|  | |
| Do the Asset Universe Granularity and Level of Detail support the Specific Purpose or our Risk Assessment (Online Banking)? | Yes, we believe the number and types of assets and the level of granularity and details support the specific purpose of this risk assessment. |
| Are there any potential observations/findings from the process of identifying the asset universe? | *Were there any assets that needed to be added to this list that you had not thought of before? For example,* Cash Management or Online Loan Applications to ensure coverage of an important focus area that may have greater risks and need other controls. |
| Identify Future Areas related to Asset Universe. | To gain the benefits from continuous improvement we identify that in the next year Mobile Banking will likely be made available to customers, we did not include it as an asset now, but will be revisiting our risk assessment before it is implemented and present a new report to the Board. Consider whether for the future it may be necessary for areas to be expanded to show a higher level of granularity. |
| Are there any areas of particular strength that should be noted for the Asset Universe? | There was a good understanding of the in-scope assets within the risk assessment or the team was not in complete agreement whether the (name an asset); for example: estatements, loan applications, bill pay, check ordering; were needed as standalone assets. |

| Universe Definition – Risks | | |
|---|---|---|
| **Methodology Steps** | | ***Project-Specific Details*** |
| | Risk Universe Granularity.<br>• How many levels of risks do we want to consider?<br>• Where will the risk list come from?<br>• What process will be used to determine the level that is appropriate for the size and | 1. *We started with the list of Risks from:* FEMA, NIST, FDIC, etc..?<br>2. *We combined the list with : …* (any other sources – the tool we used) Prior knowledge, experience, past risk assessment document, |

| Universe Definition – Risks | | |
|---|---|---|
| **Methodology Steps** | | ***Project-Specific Details*** |
| | complexity of the institution? | purchased risk assessment.<br>3. *All duplicates or irrelevant risks were exported and saved for future reference. How?*<br><br>Malicious code versus Virus versus Trojan versus Keylogger?<br>4. *We reviewed the source documents to ensure appropriate coverage.*<br>*Describe:* Our customers are all quite large, with sizable transaction volume, or very small with minimal levels? Customers are technology companies' very tech savvy or the reverse?<br>5. *The process carefully considered the appropriateness for the size and complexity of the institution while considering the Scope and Specific Purpose of this particular assessment.*<br><br>*Describe:* Didn't name every server, workstation or device. Considered groups of applications under a business area. All production servers, network rooms as one not individually. |
|  | Risk Universe Level of Detail.<br>How much information do we want to understand for each risk? This is known as "characterizing" risks.<br><br>Here is a conceptual example of a simple approach to characterization. Select a set of attributes that are appropriate for the size and complexity of the institution while supporting the risk assessment project scope and specific purpose. | 1. *We started with the attributes already identified in:* purchased software, past risk assessment, document obtained at user conference,<br>2. *We combined the list with the standard attributes from:* NIST SP800-53, COBIT, OCTAVE, ISO….<br>3. *We disabled any attributes that did not apply to the scope of the project.*<br>4. *We added additional attributes as appropriate into our tool which allows us to filter and sort based* |

| Universe Definition – Risks | | |
|---|---|---|
| **Methodology Steps** | | ***Project-Specific Details*** |
| |  | *on the risk characterization.* |
| | Do the Risk Universe Granularity and Level of Detail support the Specific Purpose?<br><br>Risk = Vulnerability + Threat | *Yes, we believe the number and types of risks and the level of details support the specific purpose of this risk assessment.*<br>*How do you Support?*<br>Industry knowledge, individual experience, training class, other experts, the examiner said so! |
| | Are there any potential observations/findings from the process of identifying the risk universe? | *We needed to add additional risks to address concepts not covered by the former risk universe. This process happened while examining the related assets and controls. We need to keep this in mind so the risk assessment process is not viewed as linear next time.*<br><br>*What did you identify while defining your Risks?*<br><br>Some Assets were unique, there were risks we hadn't thought of and we were being too granular. Train derailment was a high risk! |
| | Identify Future Areas for Risk Universe. | *It will be an ongoing challenge to identify all the different types of potential threats/risks.*<br><br>The risk universe definition process included several rounds of merging risks that had similar profiles. Given the relationships between assets and risks, this process helped focus our efforts.<br><br>*While this is not a problem, we need to make sure future assessments do* |

| Universe Definition – Risks | | |
|---|---|---|
| **Methodology Steps** | | ***Project-Specific Details*** |
| | | *not gloss over the importance of identifying specific risk areas. The example we used this time was to make sure we understood any specific risks related to:*<br>• Online Banking<br>• Wires<br>• RDC<br>• Switching Core Vendors<br>• New LOS software<br><br>In the future, we need to carefully address changes in the asset, risk and control universe (through change management and projects) as well as changes to the threat profile that directly impacts the risk universe. |
|  | Are there any areas of particular strength that should be noted for the Risk Universe? | *There was a good understanding of the in-scope risks within the risk assessment.*<br><br>*Was there?*<br><br>The Team showed strong confidence in what the purpose of this assessment was intended. A presentation was prepared for Senior Management/BOD to describe concisely and clearly where greatest inherent risk appears to be. |

| Universe Definition – Controls | | |
|---|---|---|
| **Methodology Steps** | | ***Project-Specific Details*** |
|  | Control Universe Granularity.<br>• How many levels of controls do we want to consider?<br>• Where will the controls list come from?<br><br>What process will be used to determine the level that is appropriate for the size and complexity of the institution? | 1. *We started with the list of Controls from purchased software, past risk assessment, document obtained at user conference,*<br>2. *We combined the list with the standards from NIST SP800-53, COBIT, OCTAVE, ISO….*<br>3. *We reviewed the source documents to identify* |

| Universe Definition – Controls | | |
|---|---|---|
| **Methodology Steps** | | ***Project-Specific Details*** |
| | | *expected controls for our security program.*<br>Describe: Our policy identified password controls for employees, procedures were documented for incident response and BCP/DR and tested regularly, Security awareness training.<br>4. *The process carefully considered the appropriateness for the size and complexity of the institution while considering the Scope and Specific Purpose of this particular assessment.* |
| | Control Universe Level of Detail.<br>How much information do we want to understand for each control? This is known as "characterizing" controls.<br><br>Here is a conceptual example of a simple approach to characterization. Select a set of attributes that are appropriate for the size and complexity of the institution while supporting the risk assessment project scope and specific purpose.<br>  | 1. *We started with the attributes from purchased software, past risk assessment, document obtained at user conference.*<br>2. *We combined the list with the standard attributes from methodology; NIST SP800-53, COBIT, OCTAVE, ISO….*<br>3. *We ignored any attributes that did not apply to the scope of the project.*<br><br>*We added additional attributes as appropriate which allows us to filter and sort based on the control characterization.*<br><br>*The most important was the concept _____ (for example, considering "Automated" controls.)* |
| | Do the Control Universe Granularity and Level of Detail support the Specific Purpose? | *Yes, we believe the number and types of controls and the level of details support the specific purpose of this risk assessment.* |
| | Are there any potential observations/findings from the process of identifying the control universe? | *We needed to add additional controls to address concepts not* |

| Universe Definition – Controls | | |
|---|---|---|
| **Methodology Steps** | | ***Project-Specific Details*** |
| | • Are there any controls that are known to be insufficient or non-existent in the environment?<br>• Use the source documents to see history.<br>• Use the library of controls and other guidance to see what is missing. | *covered by the former control universe. This process happened while examining the related assets and risks. We need to keep this in mind so the risk assessment process is not viewed as linear next time.*<br><br>*There were several control areas that were identified as missing or deficient. Including,*<br>_____ |
|  | Identify Future Areas for Control Universe. | *In the future, we need to carefully address changes in the asset, risk and control universe (through change management and projects) as well as changes to the threat profile and improvements in control standard-practices that directly impact the control universe.* |
|  | Are there any areas of particular strength that should be noted for the Control Universe? | *There was a good understanding of the in-scope controls within the risk assessment including any missing controls.*<br><br>*We discussed some areas of obvious strength. For example,* _____ *is a very strong control for an institution of this size and complexity.* |