### Module 5: Reader Layer

<table>
<thead>
<tr>
<th>Topic</th>
<th>Unacceptable (0)</th>
<th>Marginal (1)</th>
<th>Acceptable (2)</th>
<th>Exceptional (3)</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reader Architecture and Antenna Configurations</td>
<td>Cannot differentiate bistatic and monostatic configurations.</td>
<td>Be able to differentiate bistatic and monostatic configurations.</td>
<td>Be able to identify the two major blocks in a reader architecture.</td>
<td>Be able to differentiate sensitivity and selectivity.</td>
<td></td>
</tr>
<tr>
<td>Gen2 Sessions</td>
<td>Cannot recall how many sessions there are in Gen2.</td>
<td>Be able to recall the number of sessions in Gen2.</td>
<td>Be able to describe the purpose of sessions in Gen2.</td>
<td>Be able to choose the appropriate session for a given application.</td>
<td></td>
</tr>
<tr>
<td>Gen2 Single-, Multiple-, and Dense-Interrogator Operation</td>
<td>Cannot list two of the three operating categories of Gen2.</td>
<td>Be able to list two of the three operating categories of Gen2.</td>
<td>Be able to list the three operating categories of Gen2.</td>
<td>Be able to describe the three multiple- and dense-interrogator FDM mode methods.</td>
<td></td>
</tr>
<tr>
<td>Low Level Reader Protocol (LLRP)</td>
<td>Cannot expand the LLRP acronym.</td>
<td>Be able to expand the LLRP acronym.</td>
<td>Be able to describe the general purpose of LLRP.</td>
<td>Be able to describe the three types of parameters that LLRP can control.</td>
<td></td>
</tr>
<tr>
<td>RFID Middleware</td>
<td>Cannot define middleware.</td>
<td>Be able to define middleware.</td>
<td>Be able to describe what RFID middleware does to the tag data before sending it to an ERP system.</td>
<td>Be able to describe the advantages of using RFID middleware.</td>
<td></td>
</tr>
<tr>
<td>Reader Layer Threats, Risks, and Mitigation</td>
<td>Cannot differentiate threats and risks.</td>
<td>Be able to list some common threats.</td>
<td>Be able to evaluate risk using the STRIDE and DREAD models.</td>
<td>Be able to synthesize a new threat.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>OVERALL PERFORMANCE</th>
<th>Unacceptable</th>
<th>Marginal</th>
<th>Acceptable</th>
<th>Exceptional</th>
<th>TOTAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>POINTS REQUIRED</td>
<td>0-2</td>
<td>3-8</td>
<td>9-15</td>
<td>16-18</td>
<td></td>
</tr>
</tbody>
</table>