### Question 30 Tables and Graphics

The following are tables and graphics used in the response to Question 30.

<table>
<thead>
<tr>
<th>Risk</th>
<th>Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inappropriate access to SRS allowing DNS data to be fraudulently assigned</td>
<td>The SRS is a closed system. All access is limited to validated, certified accredited registrars who have signed contractual agreements. Once they are approved then all the factors discussed above must be in place before a registrar may interact with the registry</td>
</tr>
<tr>
<td>Unauthorized Access to Registry Data by internal users</td>
<td>Access controls have been implemented that include procedures for granting access on a need to know basis. Access control lists are periodically reviewed.</td>
</tr>
<tr>
<td>Malicious use of domains in the DNS</td>
<td>Any domain proven to be used for malicious activities are removed from the DNS or sink-holed.</td>
</tr>
<tr>
<td>Injection of malicious content</td>
<td>The registry policy engine has active validation to ensure that each data field is appropriate</td>
</tr>
<tr>
<td>Attacks on WHOIS and DNS infrastructure</td>
<td>The 24X7 network and security operation centers actively defend against general attacks form the internet.</td>
</tr>
<tr>
<td>Unauthorized Access to Data Centers</td>
<td>Each registry data center is protected using physical security controls including biometric readers. All hardware is installed with software to detect changes to the application.</td>
</tr>
</tbody>
</table>

**Table 30-1 Security Risk Mitigation**