# Examples of ‘safe and controllable’ technology

## CBRC Notice 317 criteria

The table below sets out the CBRC Notice 317 criteria for several examples of technology products and the applicable implementation schedule.

<table>
<thead>
<tr>
<th>Type of IT</th>
<th>Notable criteria for determining whether such equipment is ‘safe and controllable’</th>
<th>Implementation schedule</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(Note: Please refer above for an explanation of each of these criteria.)</td>
<td></td>
</tr>
</tbody>
</table>
| 1. Specialised banking software (including finance, risk management, e-banking, securities trading, and customer service software) | For software independently developed by the bank  
  • Domestic presence  
  • Domestic intellectual property rights  
  For jointly-developed software  
  • Domestic presence  
  • Domestic intellectual property rights  
  • Source code disclosure  
  • Regulator risk assessment  
  For software (including commissioned software) obtained from a third-party vendor  
  • Source code disclosure  
  • Regulator risk assessment  
  For both jointly developed and also third-party software, the product must be compatible with at least one other ‘safe and controllable’ hardware product or systems software product (such as the operating system, data storage application, and/or middleware). | 5–15 per cent  
(15 per cent for major banks, 10 per cent for smaller regional banks and credit associations, and 5 per cent for other financial institutions) |
| 2. Remote access and other virtualisation software | • Source code disclosure  
• Domestic presence  
• Regulator risk assessment | 10 per cent |
| 3. Middleware | • Source code disclosure  
• Domestic encryption technology  
• Domestic presence  
• Regulator risk assessment | 30 per cent |
| 4. Software tools (including network security, coding, project management, data management, CAD and graphics design software) | • Source code disclosure  
• Domestic encryption technology  
• Domestic presence  
• Regulator risk assessment | 15 per cent |
| 5. Routers and network switches | • Source code disclosure (for accompanying software and firmware)  
• Domestic encryption technology  
• Domestic presence  
• Regulator backdoor  
• Regulator risk assessment  
• Domestic intellectual property rights  
(this requirement applies to routers only) | 75 per cent |
<table>
<thead>
<tr>
<th>Type of IT</th>
<th>Notable criteria for determining whether such equipment is ‘safe and controllable’</th>
<th>Implementation schedule</th>
</tr>
</thead>
<tbody>
<tr>
<td>6. Wireless LAN equipment</td>
<td>• Source code disclosure (for accompanying software and firmware) • Domestic encryption technology • Domestic presence • Regulator backdoor • Regulator risk assessment • Domestic intellectual property rights</td>
<td>75 per cent</td>
</tr>
<tr>
<td>7. Storage equipment (including storage fibre channel switches, disk arrays, etc.)</td>
<td>• Source code disclosure (for accompanying software and firmware) • Domestic encryption technology • Domestic presence • Regulator backdoor • Regulator risk assessment • Domestic intellectual property rights</td>
<td>50–80 per cent, depending on the specific type of equipment</td>
</tr>
<tr>
<td>8. Firewalls</td>
<td>• Source code disclosure (for accompanying software and firmware) • Domestic encryption technology • Domestic presence • Regulator backdoor • Regulator risk assessment • Domestic intellectual property rights</td>
<td>100 per cent</td>
</tr>
<tr>
<td>9. Mainframes</td>
<td>• Domestic encryption technology • Source code disclosure (for accompanying software and firmware) • Regulator risk assessment</td>
<td>0 per cent (however, banks must develop plans to migrate to other (non-mainframe) solutions)</td>
</tr>
</tbody>
</table>