

# Enter Internal Review Notes

Use the **Internal Review Notes** section to specify text or questions that IDERA SQL Secure should include in your Risk Assessment and Assessment Comparison reports. These notes can serve as a questionnaire to be used for manually gathering additional data that may be required in your assessment.

The screenshot shows the 'SQL Secure Create Policy' window with the 'Internal Review Notes' tab selected. The window has a title bar with standard Windows controls. Below the title bar, the 'Internal Review Notes' section is titled 'Specify any additional information that should be included in the policy report.' and includes a globe icon with a green plus sign. A text box contains the instruction: 'Text can be added to your security assessment report to enable manually gathering data and reporting it in one comprehensive place. Enter an optional title and additional text for your report here.' Below this is a 'Title' label and a text input field containing 'CIS Interview Checks'. A large text area contains the following text: 'Benchmark for Microsoft SQL Server 2000, Version 1.0, December, 2005' followed by numbered items 1.1 through 1.7. At the bottom left of the text area is a 'Check Spelling' button. At the bottom right are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

**Internal Review Notes**  
Specify any additional information that should be included in the policy report.

Text can be added to your security assessment report to enable manually gathering data and reporting it in one comprehensive place. Enter an optional title and additional text for your report here.

Title  
CIS Interview Checks

Benchmark for Microsoft SQL Server 2000, Version 1.0, December, 2005

1.1 Physical security Place the SQL Server in an area where it will be physically secure. Place the server where only authorized personnel can obtain access.

1.3 SQL Servers accessed via Internet  
If the SQL Server is being accessed via the Internet, place the SQL Server inside a DMZ with the Web Server.

1.4 SQL Servers accessed via Internet - Put a firewall between your server and the Internet.  
In a multi-tier environment, use multiple firewalls to create more secure screened subnets. Consider separating Web logic and business logic onto separate computers.

1.5 IPSEC - Use IPSEC policy filters to block connections to ports other than the configured SQL Server ports. IPSEC offers authentication, integrity, confidentiality, and anti-replay services. SSL can provide these services for all database connections; however, IPSEC can allow these services to be configured on selected computers and ports.

1.6 Encryption - Implement SSL. Use the fully-qualified DNS name of the server in the certificate to help prevent masquerading.

1.7 Test and development servers - Maintain test and development servers on a separate network segment from the production servers. Test patches carefully before applying them to production systems.

Check Spelling

< Back Next > Cancel Help



You can use the option **Check Spelling** to make sure the information displayed on your report is well written.

Click **Next** to go to the Completing SQL Secure New Policy Wizard section.

[IDERA Website](#) | [Products](#) | [Buy](#) | [Support](#) | [Community](#) | [About Us](#) | [Resources](#) | [Legal](#)