

Question 30 Tables and Graphics

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

Risk	Mitigation
Inappropriate access to SRS allowing DNS data to be fraudulently assigned	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
Unauthorized Access to Registry Data by internal users	Access controls have been implemented that include procedures for granting access on a need to know basis. Access control lists are periodically reviewed.
Malicious use of domains in the DNS	Any domain proven to be used for malicious activities are removed from the DNS or sink-holed.
Injection of malicious content	The registry policy engine has active validation to ensure that each data field is appropriate
Attacks on WHOIS and DNS infrastructure	The 24X7 network and security operation centers actively defend against general attacks from the internet.
Unauthorized Access to Data Centers	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.

Table 30-1 Security Risk Mitigation