24/7

IS Security & Architecture Specific Questions

IS Security

The external hosting of the service

1. What physical security measures are in place in offsite? This should cover policies and procedures, site, building and room where staff is supported. Details should cover security guards, checks, use of swipe cards, and procedures on checking electronic devices and media as well as paper media.

5/w 24/w

2. What support model will be proposed? This should cover number of personnel, level of qualifications, background checks undertaken for such personnel staff, shift basis, and working location (including remote sites away from main offices, i.e., home working). Does the company support other clients and systems? Is the company ISO 17799 compliant?

3. Describe the security architecture and controls. This should include any logical perimeters proposed at the location (such as routers, VLANS, and firewalls), level of authentication and encryption, and level of auditing and intrusion detection. Again, as mentioned, it would be great if they could provide independent assurance/reports/certificates on external penetration tests conducted.

4. Describe the security configuration of the desktops or laptops that will be used by support personnel. This should include software (and their versions) used to protect against virus, Spyware and other malicious code, device firewalls and any IPS systems. Additional information such as patching and AV signature updates would be useful. If email and internet access is permitted on such devices, then details on AV and proxy settings and content filtering should be given.

5. What disaster recovery arrangements are in place? This should cover personnel, locations, system resilience and redundancy, type of standby arrangements, timescales, network and remote connections, testing, backup and environmental conditions.

6. We need to ask about protection on these servers: OS versions, patching, vulnerability testing, user accounts and privileges, and monitoring. I can't imagine they'd let us check the health of their environment by conducting a vulnerability scan. However, again if they can produce some independent assurance/report that would be great.

The web application itself

Concerns related to key problems in code development which can be categorised as:

- Weak file and group permissions
- Race conditions
- Buffer overflows
- Problems with temporary files
- Overly complex and unnecessary code
- Insecure system calls and switches
- Hard-coding passwords

& "password distribution" guidelines.

Technical Architecture / Hosting arrangements (Infrastructure aspects that affect NG directly)

Assuming that you are going for a Hosted service then we will need to understand:

- How the service is accessed from the National Grid network?
- Are there any additional hardware or software components needed within our infrastructure to support access to the service?
- What are the bandwidth requirements needed to support the National Grid user base?
- Who manages the administration of the service? (Account creation/deletion, Password resets, Audi, Archive & backup processes etc.)

An over view of the proposed hosted service would be helpful in understanding and validating the responses to the above questions.