Vendor evaluation questions

In a cyber environment with ever-changing risks and threats, it is important that your organisation maximises its investment in its security technology. This means not just having a complete understanding of the pros and cons of the solution itself but also of the vendor's own understanding and expertise.

Many vendor-related problems can be avoided if you take the time to research a provider before committing to a particular solution. To help you avoid these problems, your organisation's assessment of a security solutions should be based on the following pillars:

Plan ahead: Understand what your vulnerabilities are in terms of IT and future business requirements

Scale up: Ensure the selected security solution can handle your company's emerging needs

Complete offering: Look into the range of technologies available by the vendor and ensure they can offer you and end-to-end solution that comprises of the best technologies available.

Organisations that find themselves in the process of identifying a security solution encounter a myriad of technologies, problems and obstacles during the buying process. The questions below provide practical advice to help avoid mistakes than can cost your organisation a lot of time and resources and will help you go beyond the technology and evaluate the knowledge, experience and commitment of the vendor.

Top **5** questions:

Will you work with us to review and health-check our overall security strategy rather than just recommending products?	no ☐	yes ☐
Will you bring all the different components of the solution together and take responsibility for ensuring we know when new versions are released.	no ☐	yes ☐
Do you have specialist licensing expertise to ensure we are compliant but not overlicensed?	no ☐	yes ☐
Do you have strong and proven partnerships with market - leading security vendors? Do you always recommend their solutions or do you also use smaller "niche" specialists if appropriate?	no ☐	yes ☐
Will you help us prepare for the aftermath of a breach so we can contain its impact?	no ☐	yes ☐

Insight