Questions to ask when

Evaluating a Compliance Management System

When organisations engage a H&S systems provider, they are entrusting them to safeguard sensitive documents and provide a system for sharing access to those documents. This trust goes beyond technical specifications.
To that end, here are a few questions that organisations should be asking of any H&S Compliance solution provider:

1. **IS THE PROVIDER TRANSPARENT ABOUT ITS SECURITY PROCESSES?**
The provider should be clearly able to explain its physical security safeguards (protection of the servers, routers and other equipment), screening processes for new hires, internal controls, system monitoring (if they were hacked, how would they know?), and any history of security breaches and their resolution.

2. **DOES THE PROVIDER MEET THE HIGHEST INDUSTRY STANDARDS?**
As third-party handlers of confidential information, one should meet security standards comparable to those of the most demanding IT departments across a number of industries. Key accreditations include: a history of clean annual audits (covering how providers report on their internal controls) and ISO 27001 certification for security (compliance of the actual software provider's information security management systems with international standards, as opposed to merely their data hosting centres' compliance).

3. **DOES THE PROVIDER ALLOW OUTSIDE PENETRATION TESTING?**
Do most providers conduct penetration testing as part of their quality control?. Compliance management solutions with high security standards will conduct testing on an almost continuous basis in order to keep up with evolving threats. They should also allow 3rd parties to conduct their own security and to run independent tests. Doing so is a powerful demonstration of confidence – as well as an acknowledgement that security is ultimately a team effort.

4. **DOES THE PROVIDER RELY ON THIRD PARTY PLATFORMS OR SOFTWARE?**
Many H&S compliance systems are built on top of commercially available platforms, or they use ready-made plug-in components for certain elements of their software. Those third-party elements, however, come with their own security vulnerabilities, which are attractive to hackers precisely because those platforms are so widespread . Instead, compliance management systems should be built from the ground up with security features designed into the applications at every point.

5. **WHAT ABOUT USERS WHO ARE LESS COMFORTABLE USING TECHNOLOGY?**
A compliance system provider should provide extensive customer care that includes one-on-one training customised to each person's experience and comfort level. In addition, Once the late adopters see from watching their peers how easy it is to use, they will invariably make the transition at their own pace.

6. **WHAT DEGREE OF REDUNDANCY IS PROVIDED?**
Is data backed up and do primary data centres fail over to disaster recovery data centres? providers must offer remote, geographically dispersed locations to ensure that any event impacting one location will not affect the secondary location. In addition, data redundancy must be supported by real-time, 24/7 intelligence on data performance

7. **CAN USER ACCESS TO THE SYSTEM BE RESTRICTED?**
With user base spread around the country and possible different sites, the need for securing their information at different levels is paramount. Can a user access to the system be restricted to a different tiers/levels/sites/positions? The result is stronger control of access rights.

8. **DOES THE PROVIDER ALLOW YOU TO CUSTOMISE THE LEVEL OF SECURITY?**
Every security solution involves a trade-off between convenience and security. As a result, one size definitely does not fit all organisations. Instead, it should be able to tailor functions to fit an organisation's specific security needs, such as allowing for different password strengths, lockout policies, and options for exporting or sharing documents at different levels.

9. **ARE THE SYSTEMS SECURITY FEATURES BACKED UP WITH CUSTOMER SUPPORT?**
No matter how strong a systems security may be, human monitoring is needed to ensure that any issues are dealt with promptly. Both to provide assistance and support as and when needed with a proactive approach. Local support 24/7 is critical.

HSEC onLINE®
Simple. Smart. Safe.

Saryx
ENGINEERING GROUP (PTY) LTD