YOUR CYBER-SECURITY CHECKLIST

Below are the top **10 software asset management actions** you can take to minimise your organisation's cyber risks.

☑ **1.**
Get the buy-in of top the management of your organisation for software asset management

☑ **2.**
Have clear roles and responsibilities; while one person should be accountable for cyber-security, ALL employees and IT staff need to be clear on their obligations when it comes to cyber security

☑ **3.**
Develop written policies that cover the procurement, maintenance and decommissioning of software and cloud services

☑ **4.**
Have a specific 'acceptable use' policy for non-IT employees so they are clear about their responsibilities for looking after IT equipment, requesting software and cloud services and using IT systems and services

☑ **5.**
Don't give employees administrator rights on their IT equipment; this will limit their ability to download and install unlicensed or privately purchased software

☑ **6.**
Only procure software from legitimate sources which are certified by the software publisher

☑ **7.**
Keep records of all the hardware and software that you own as well as your cloud services subscriptions. Specialist IT Asset Management tools can act as a data repository for IT asset records and help reconcile your records of what you own and what you are using

☑ **8.**
Regularly audit the hardware, software and cloud services in use within your organisation

☑ **9.**
Check that software is patched and maintained on a regular basis, and that all machines have anti-virus software installed

☑ **10.**
Identify unused, old and obsolete software (again, an IT Asset Management tool can help with this), delete what you can, and work with employees to migrate older systems onto upgraded or replacement systems where needed