Frequently **A**sked **Q**uestions on

ISO27k (the ISO/IEC 27000 family of information security standards)

Q. Does ISO 27001 apply to us?

A. Yes. ISO/IEC 27001 and other "ISO27k" standards recommend information security practices for all kinds and sizes of organization - commercial businesses, not-for-profits, charities, government departments, multinationals, corner shops and more.

Q. How does that work?

A. The standards explain how to identify and deal with information risks systematically. Unlike, say, PCI-DSS (the IT security standard for organizations accepting bank and credit cards), the ISO27k standards don't specify which information risks to address, and they only *suggest* how to go about tackling them in general terms (*e.g.* selecting appropriate security controls similar to those suggested), giving organizations plenty of flexibility in how to use the standards in practice.

Q. With so much flexibility, how can organizations be certified?

A. ISO/IEC 27001 carefully specifies the 'management system' with which organizations manage their information risks and information security controls. The specification is so detailed and explicit that auditors can determine whether organizations are conformant, meaning that they have the specified policies and processes in place to identify, assess, evaluate and treat their information risks, to handle incidents competently and to improve their arrangements continuously. Improvement is an important part of the ISO27k approach; no matter how strong the organization's information security is right now, there are always opportunities to make it even better.

Q. What's in it for us?

A. Using the ISO27k standards brings *many* benefits to the business *e.g.* assurance; availability of information; baseline; brand-enhancement; business continuity & drive; clarity & focus; competence; compliance; comprehensive; confidentiality; continuous improvement; control; demonstrable practices; due care; effectiveness; efficiency; financial & non-financial benefits; flexibility; good practice; governance; independent benchmark; information risk management; integrity; international; knowledge; maturity; measurable; optimization; oversight; planning; pragmatic; privacy; proactive; proportional protection; raises-the-bar; reputation-enhancing; resilience & strength; risk-alignment; safety & security; strategic, tactical *and* operational benefits; structured, rational, systematic and rigorous; traceability; transparency; trustworthiness; universal applicability; validation; widely-recognised; exemplifies a modern, proactive approach; yardstick; year-round effort; zero trust. A management briefing explains these plus the costs and downsides of ISO27k (yes, there are some!). Browse www.ISO27001security.com

Q. Why does it concern *me*?

A. We *all* use and depend on information. We *all* face information risks and need information security, privacy, safety and so on. ISO27k helps us handle all of that competently and professionally … and we *all* have our parts to play.

Further information

Speak to your manager, browse the intranet *Security Zone*, or contact the Help Desk.