Flex-Protection Bullet Point Briefing: ISO 27001

The following simplified briefing will not make you an expert on the ISO 27001 requirements and documentation. But it should help you decide if you want to embark on a project to obtain this well-known certification.

1) What is it? (ISO 27001 is a global standard which specifies the implementation of policies, procedures, and controls which constitute an Information Security Management System (ISMS).

2) ISO 27001 is intended to evaluate and validate your ISMS. Your ISMS is not a software package, but essentially a collection of procedures, requirements and controls, and lots of documentation.

3) The ISMS is designed to protect an organization's operating and financial data wherever it resides (including interfaces and databases controlled by business partners and third parties). It is very much part of the cybersecurity world.

4) Pursuing an ISO 27001 certification will add work, cost, and certainly new/revised documentation. There is no denying it. HOWEVER, you can decide on the scope of your certification; it need not cover all your operations, locations and products/services.

5) Who needs ISO 27001? Larger companies and organizations, certainly, but also those whose customers require it. Over time, your needs may change.

6) You need to establish a Governing Body. This is a fancy way of saying that someone from your top management team, and perhaps several executives, needs to be involved in the project, in a visible way.

7) The ISO 27001 standard has the formal name of "ISO/IEC 27001:2013", and includes components such as ISO 27002, and others. ISO 27002, also known as "Annex A", refers to the actual documents and tools implemented in the ISMS, while "ISO 27001" refers to the standard itself.

8) A successful ISMS achieves three objectives for your critical data, known as the CIA triad. The objectives are Confidentiality (authorized users only), Integrity (not altered or damaged, and Availability (ready when needed). It does not matter if the data is on paper, in the cloud, on your network, or on portable devices.

9) ISO 27001 enhances information security and helps organize and validate your processes and procedures. But its real purpose may be as a marketing tool. Having the certification is considered a recognized achievement and thus allows you to advertise your compliance, which therefore creates a business advantage.

10) ISO 27001 is technology and vendor neutral and fits all industries and organizations of any size. Its cornerstone is an Information Security Policy, which you will create, and which lays the foundation for the policies, procedures and controls that follow in your ISMS.

11) The cost and duration of a certification initiative varies widely based on company size, operational complexity, and other factors. It is NOT an IT project – you can expect to allocate resources – people and time – from multiple departments and top management.

12) Implementation generally follows a simple outline, referred to as "PDCA" or Plan, Do, Check, and Act. Planning is key, and is followed by implementation, monitoring the ISMS, and acting to make corrections. It should be an iterative process, with regular improvements.

13) Annex A (or ISO/IEC 27002:2013) contains the actual "controls" (114 of them, divided into 14 "domains"). You will need to become familiar with this list early in the process. It is not included here.

14) Within Annex A, you do not need to utilize every control and every document. You may choose which tools and documents you want to include. However, you are expected to create a "Statement of Applicability" that describes why certain controls were included and otherers were not.

15) Management support and review must be in place in order to pass a certification audit, which is the whole point of all the additional work and expenditure.

16) Choosing controls to implement and document may be thought of as a Risk Management exercise, It is important to estimate costs, identify benefits, and choose controls based on cost/impact.

17) When addressing risk with defensive measures or operational controls, for each risk identify one of four strategies: Avoid, Accept (small risks), Mitigate (with defenses) or Transfer (to someone else).

18) You must conduct an Internal Audit to evaluate your ISMS. At this point you will self-verify, to reduce or eliminate surprises which may occur in the External Certification Audit to follow.

19) Your internal audit may be conducted by staff or by a third party. It will be followed by an external audit, in two stages.

20) External Audit - Stage 1: Largely a deep documentation review. You should ask your auditor in advance "What documentation will you look for?"

21) Your auditor may pause the audit after Stage 1, to allow you to make substantial corrections or improvements before proceeding to Stage 2.

22) External Audit - Stage 2: Making sure your ISMS actually conforms to ISO 27001. If successful, you can now advertise that you are "certified".

23) Non-conformities will be identified during your internal audit and possibly in your external audit. (ex: a broken process, ignored procedures, missing documentation). You will need to address each of these (with proof of follow-up, who, when, etc.)

24) Audits are done on a 3-year cycle. In other words, to keep your certification current, you must conduct the external audit every three years.

25) ISO Service Providers / Consultants are available for projects of all sizes. You can expect to spend between $10,000 and $50,000 USD in professional services fees for support, guidance, and audits.

26) The ISO 27001 certification is considerably different from the also-popular "SOC 2" certification. You may wish to consider both options before investing in either.

Conclusion: Expect some investment of time and money to accomplish this highly-regarded certification. It's not for everyone.

If you decide not to pursue an ISO 27001 certification at this time, please consider the following simple measures to enhance your data security:

1) Make a list of all your data stores/files, including where they live (servers, desktops, portables, home offices), expected damage if lost or breached, and how they are being protected.

2) Automate and verify your daily and weekly backups (to help you survive a successful ransomware attack). Suggest critical data be kept on servers, simplifying backups.
3) Conduct some form of User Security Awareness Training at least annually (include better awareness, latest policies, updated procedures, a security mindset, password management, safe browsing).
4) Make a list of names and phone numbers for everyone you need to contact when a security incident occurs, and post it where it can be seen. This is your bare bones “Incident Response Plan”.
5) Consider getting some help, such as an assessment, policy review or user training from a professional.