

ISO/IEC 27001

Implementation Tips and Tricks

Mark Dearlove – Security & Compliance
Officer



Its all about me....



IT Industry since 1998

- Software Developer
- System Administrator
- Penetration Tester
- ISMS Implementer
- Security Research

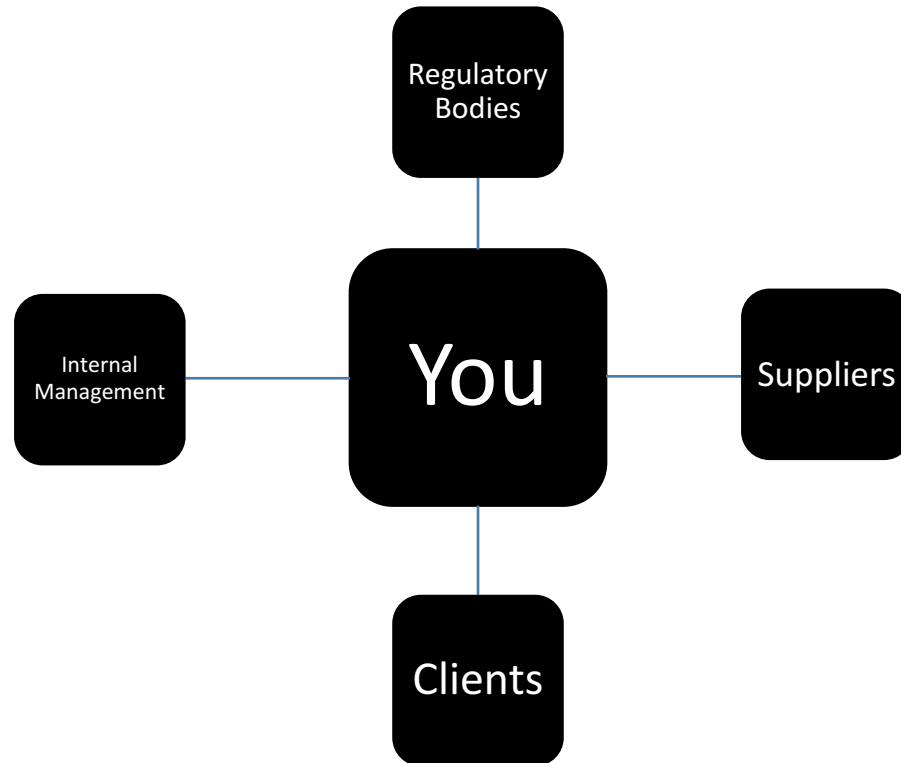
Firstly.....



Have you considered?

- ✓ Understand why you require ISO/IEC 27001
- ✓ Do you have the resources needed
- ✓ Costs – staff training, software, document toolkits and certification
- ✓ To certify or not to certify – that is the question

Understand why you require ISO/IEC 27001



Costs - Do you have the resources needed?

- ✓ Management backing
- ✓ ISO 27k Implementer (5 day course)
- ✓ ISO 27k Internal Auditor (3 day course)
- ✓ Additional resources if you are a large organisation

Costs - A little help from software

- ✓ Death by paperwork! – Don't write the ISMS documents from scratch – you only live once! – Buy a documentation toolkit
- ✓ Information Assets and Risk assessment – Software to track the assets and provide reporting with key ISMS docs like – SOA, RTP - Could be a one user system or many depending on your organisation size
- ✓ Staff Education – InfoSec Awareness E-learning resources – **DON'T UNDERESTIMATE THIS WORK – IT CAN BE VERY CHALLENGING TO GET STAFF ENGAGED!**

What does it cover?



Interactive
ITP

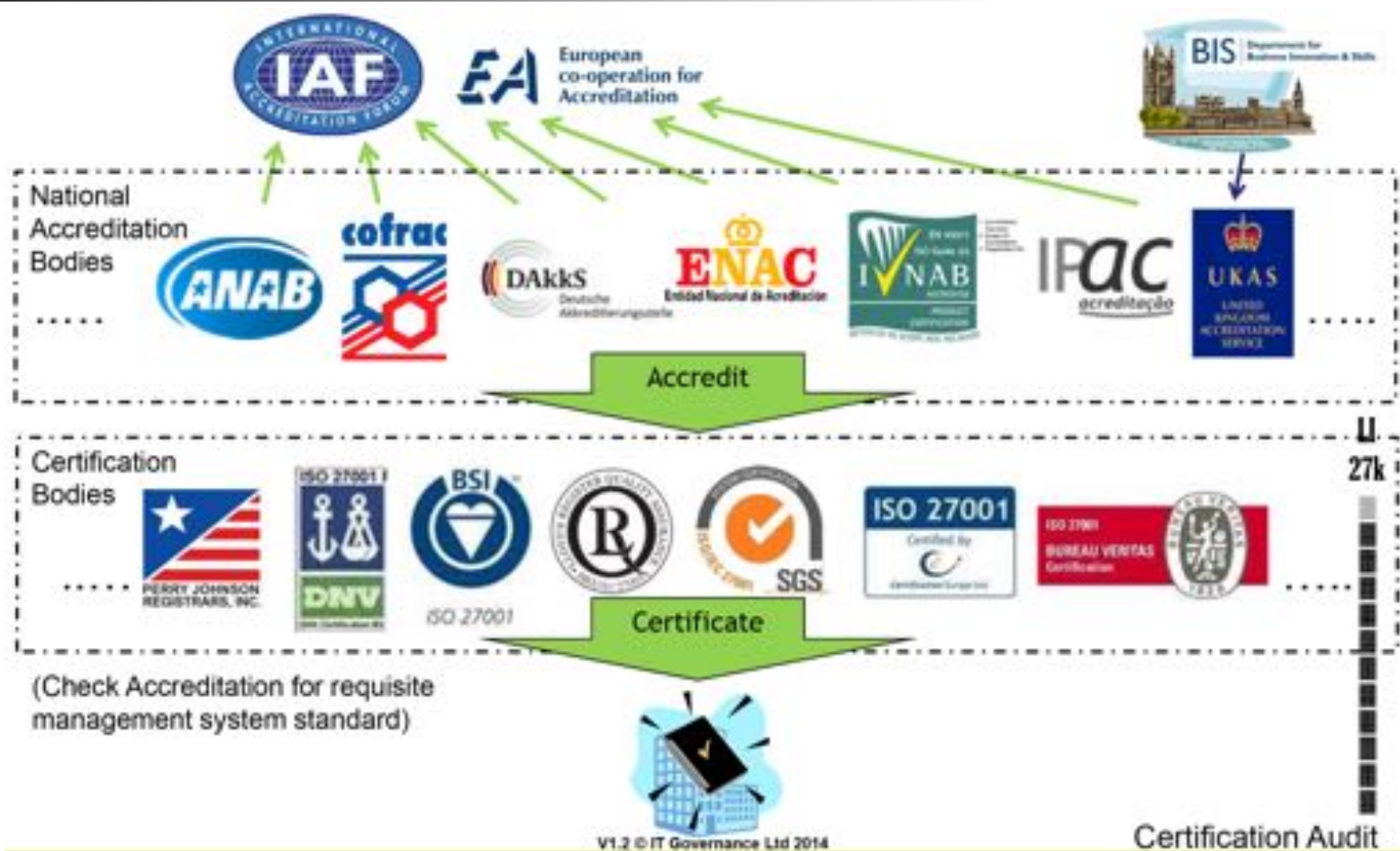
To certify or not – the options

Accredited Certification

Certification

Adopt

Accredited Certification - Who's who



Certification Audit Insight

- Stage 1 Audit – are the basics in place in the organisation? Will check that all the sections of the standard have relevant documentation and policies
- Leave a gap of 5 week-ish for potential remediation work
- Stage 2 Audit – Deeper look at policies and documents/evidence and interviews with staff
- Surveillance visits – ensure that you are doing what you say you are doing in your policies