One Standard to Rule Them All

Using ISO/IEC 27001 to manage your compliance with other information security standards

Bridget Kenyon
Head of Information Security
UCL

Chair
BSI Panel 1

Things I'll be talking about

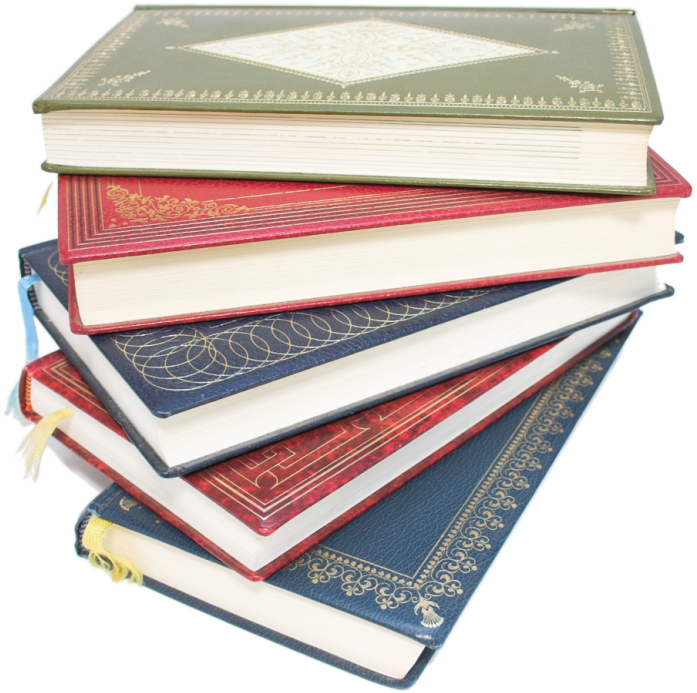
1. What's the problem?
2. Why add 27001?
3. How it worked for us
4. Some general tips

What's the problem?

Too many standards

PCI DSS

Cyber Hygiene Profile



IGTK

RIPA

DPA

SOX

Too little time

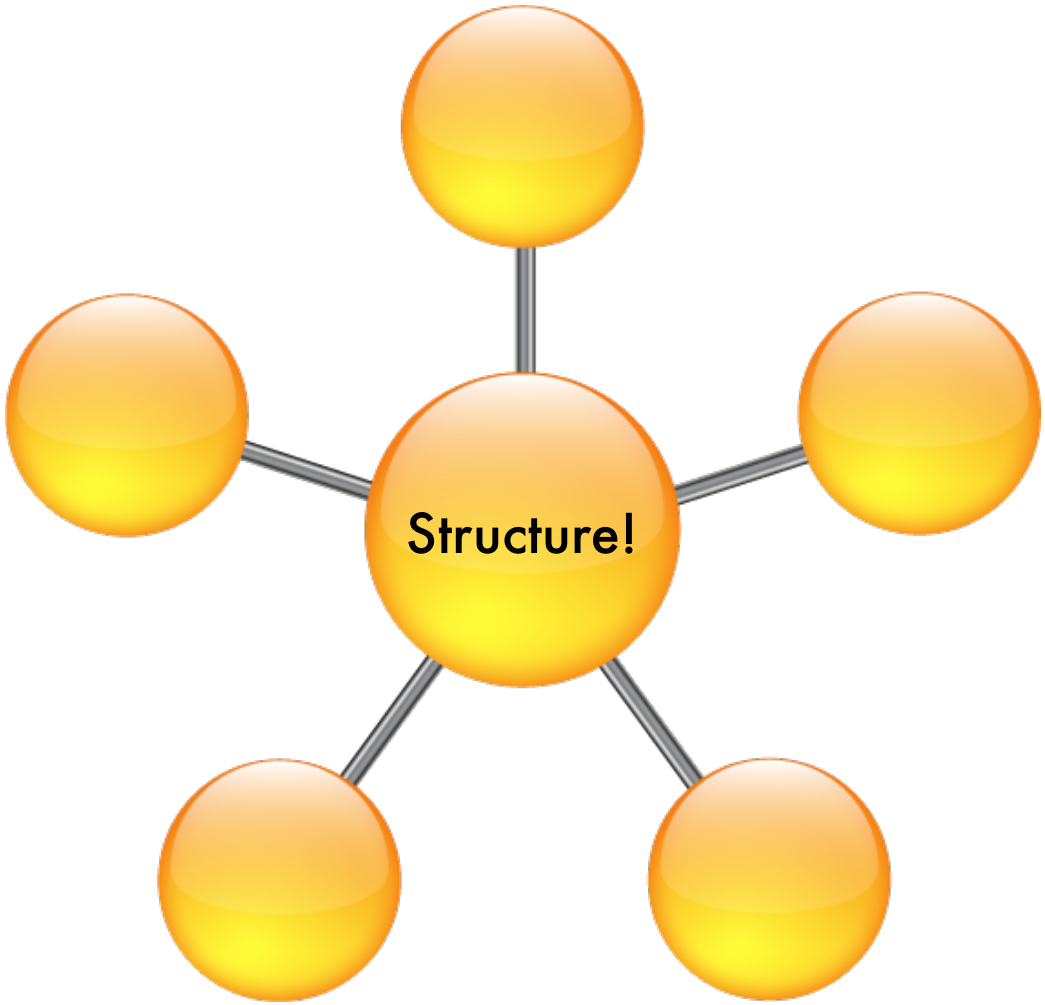
Focus on ticking boxes

Why add 27001?

What do we want?

- Protection from risk
- Prevention of reputational damage
- Ability to support business activities

What do we need?



27001 provides

- A framework for managing external requirements for information security
- A way to combine this with local risk appetite
- A blueprint for decisions about handling risk
- Instructions for creating business processes

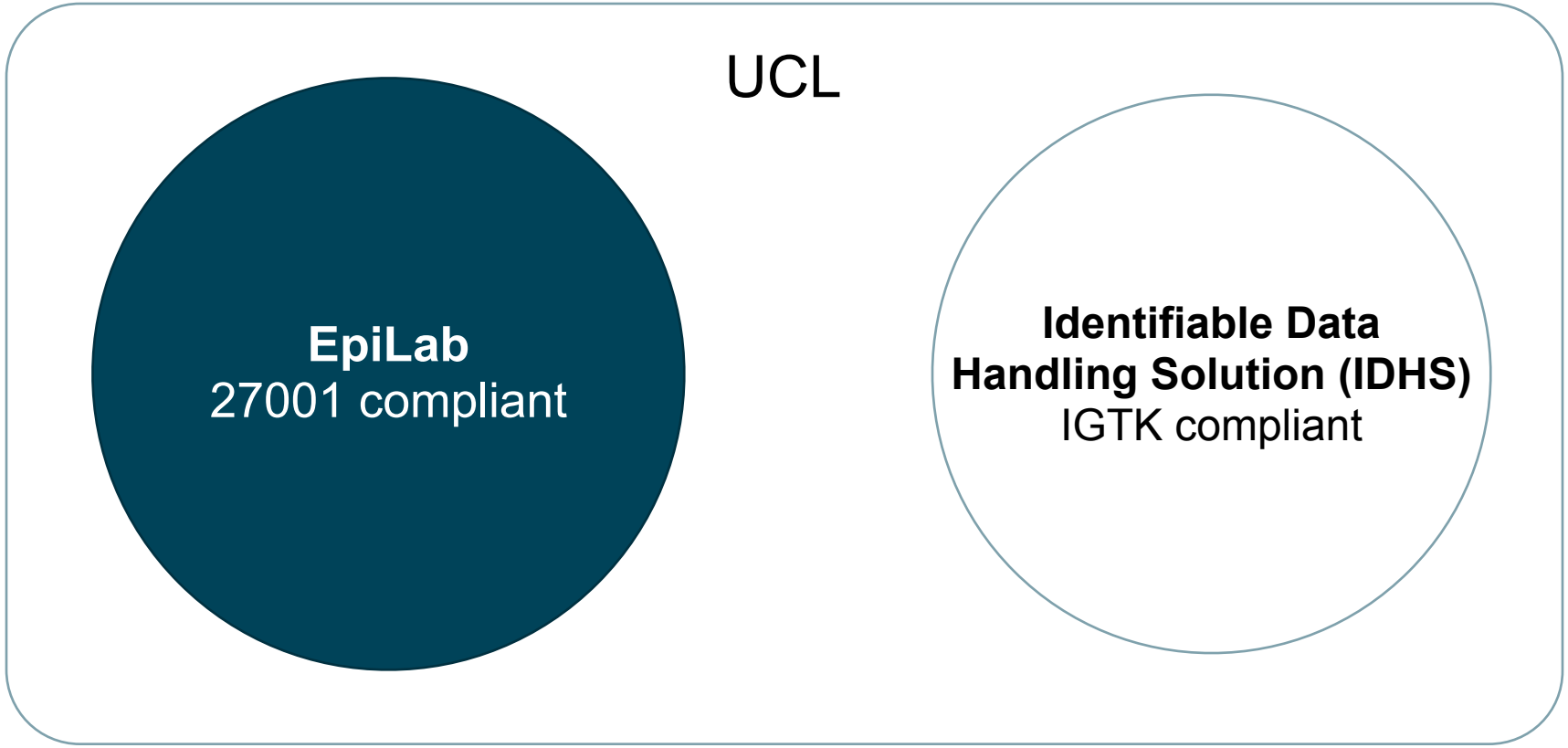
Add 27001 to get:

Indicators

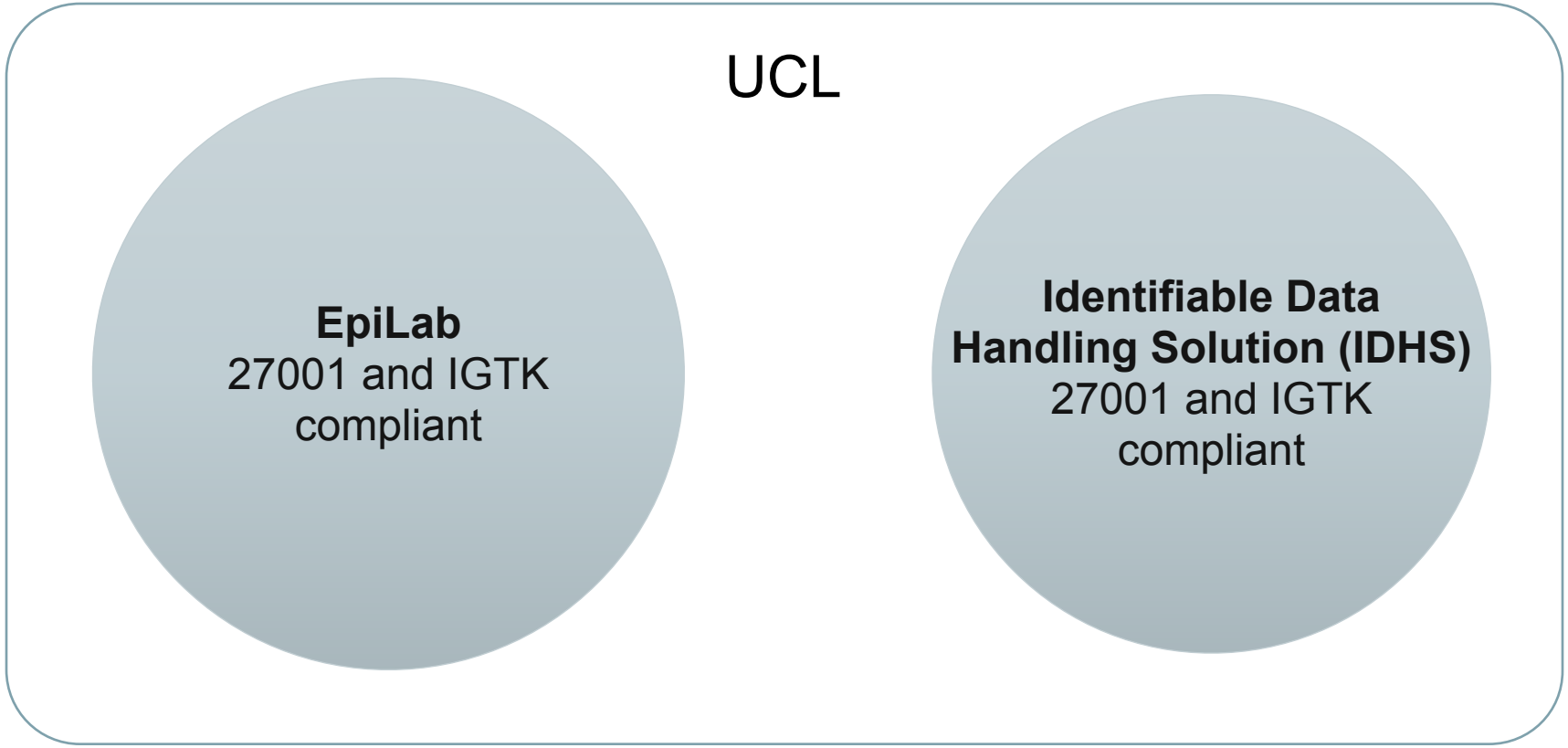
- More than one standard
- Standards relate to information security
- Formal reporting requirements
- Sensible scope
- Top level buy-in

How it worked for us

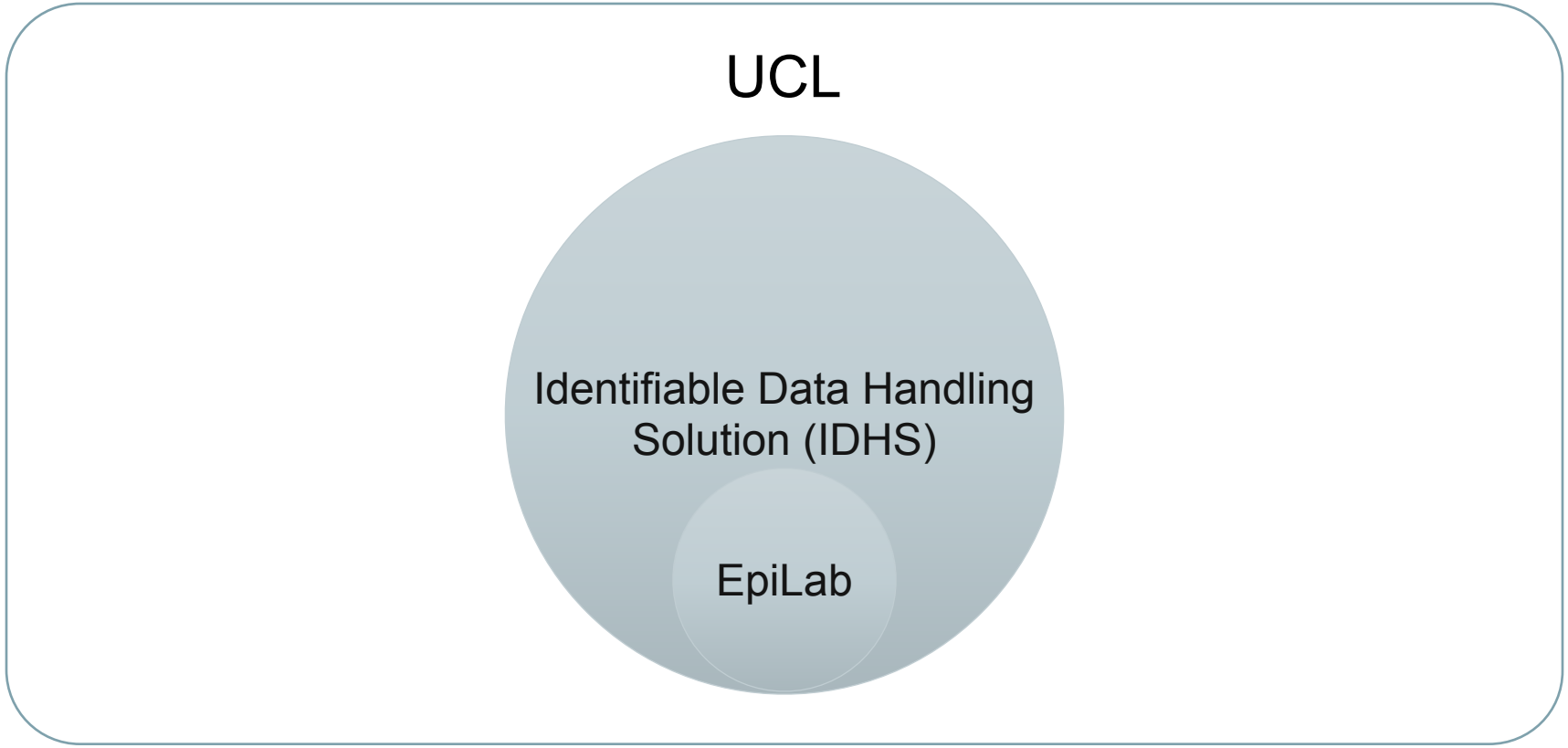
Our situation



Our decision: now



Our decision: next



Approach to 27001 adoption

- Running as a phase in overall IDHS project
- Using external consultant
- Collaboration with central information security
  - Linked management structure
  - Acting as internal audit
- Standard list of 11 risks

Progress

- EpiLab compliant with IGTK (took 3 months)
- IDHS due for 27001 audit in May

Lessons learnt so far

- Scope is very challenging
- Raises awareness
- Quite a lot of tying things together
  - Governance in place
  - Policies generally already done
  - Training sorted
  - Most necessary controls already implemented
  - Needed risk assessment

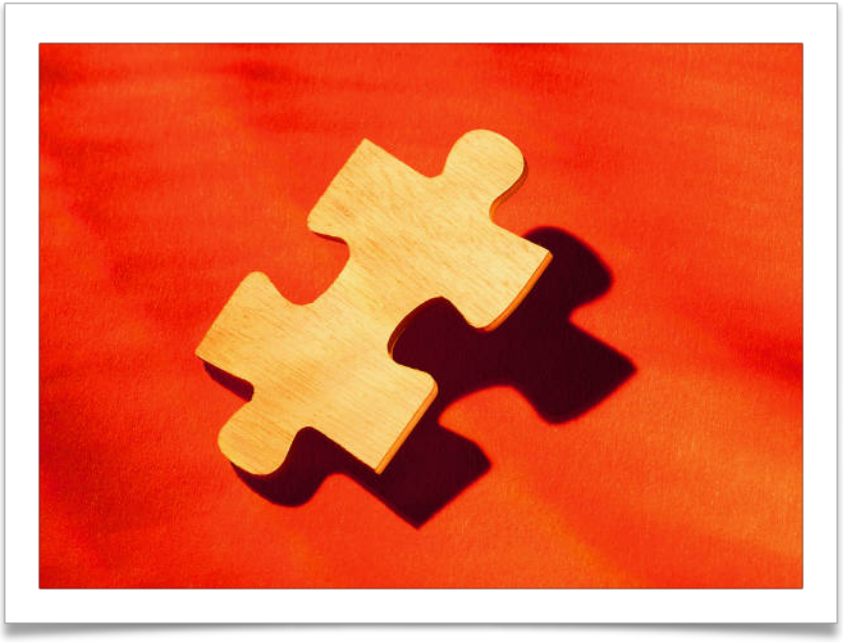
Tips

Things to bear in mind

- Get some training
- Consider professional assistance
- Agree scope
- Gap analysis
  - Map between each standard and 27001
- Retrofit controls
- Paperwork is no longer king
- Internal audit in parts
- External audit is a constructive process

Most importantly...

- YOU ALREADY HAVE AN ISMS!



Finally- should you certify?

- Yes! Totally different level of rigour between "conforming to" a standard and certifying to it.