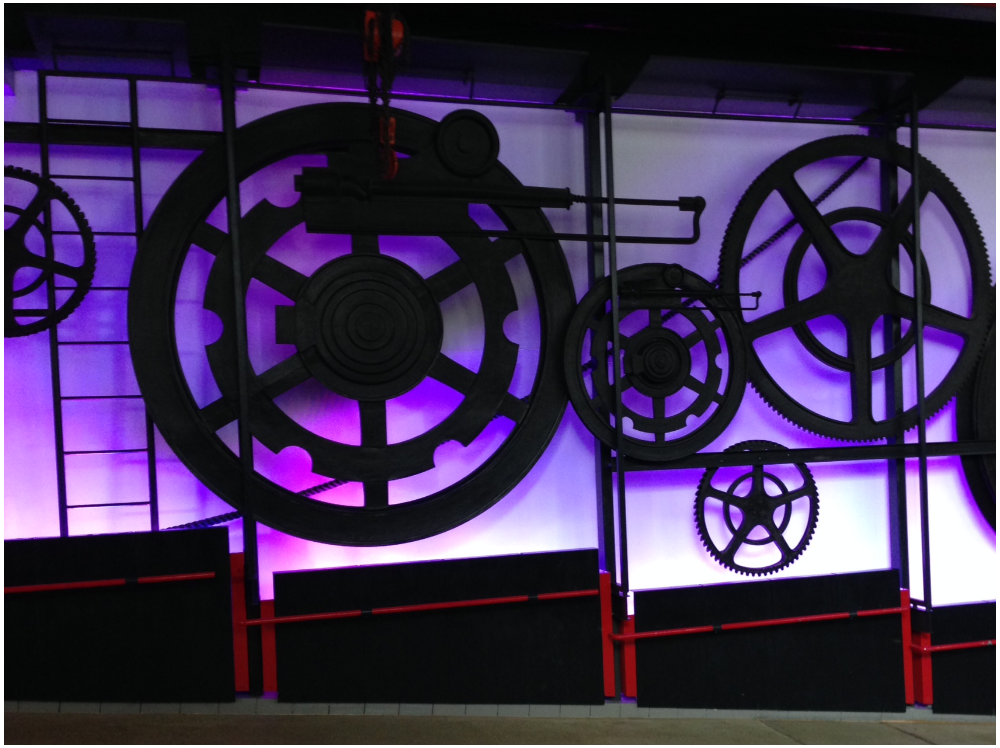
Alignment of IGTK and ISO/IEC 27001

How to get there from here



Bridget Kenyon

- *Head of Information Security,UCL*
- *Chair, IG Working Group*
- *Chair, BSI Panel 1*

Things I'll be talking about

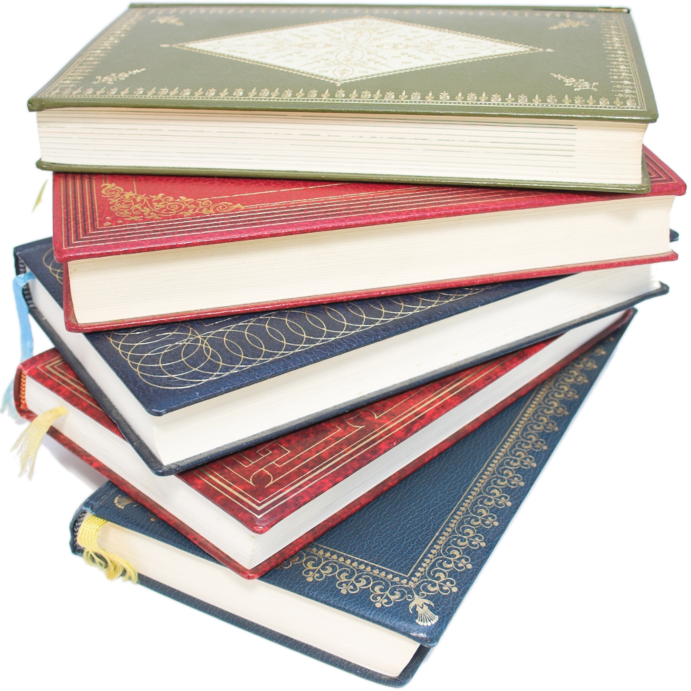
1. Background
2. Why both standards?
3. How it worked
4. Some general tips

Background

Too many standards

PCI DSS

Cyber Essentials/
Hygiene



IGTK

RIPA

DPA

SOX

Too little time

Focus on ticking boxes

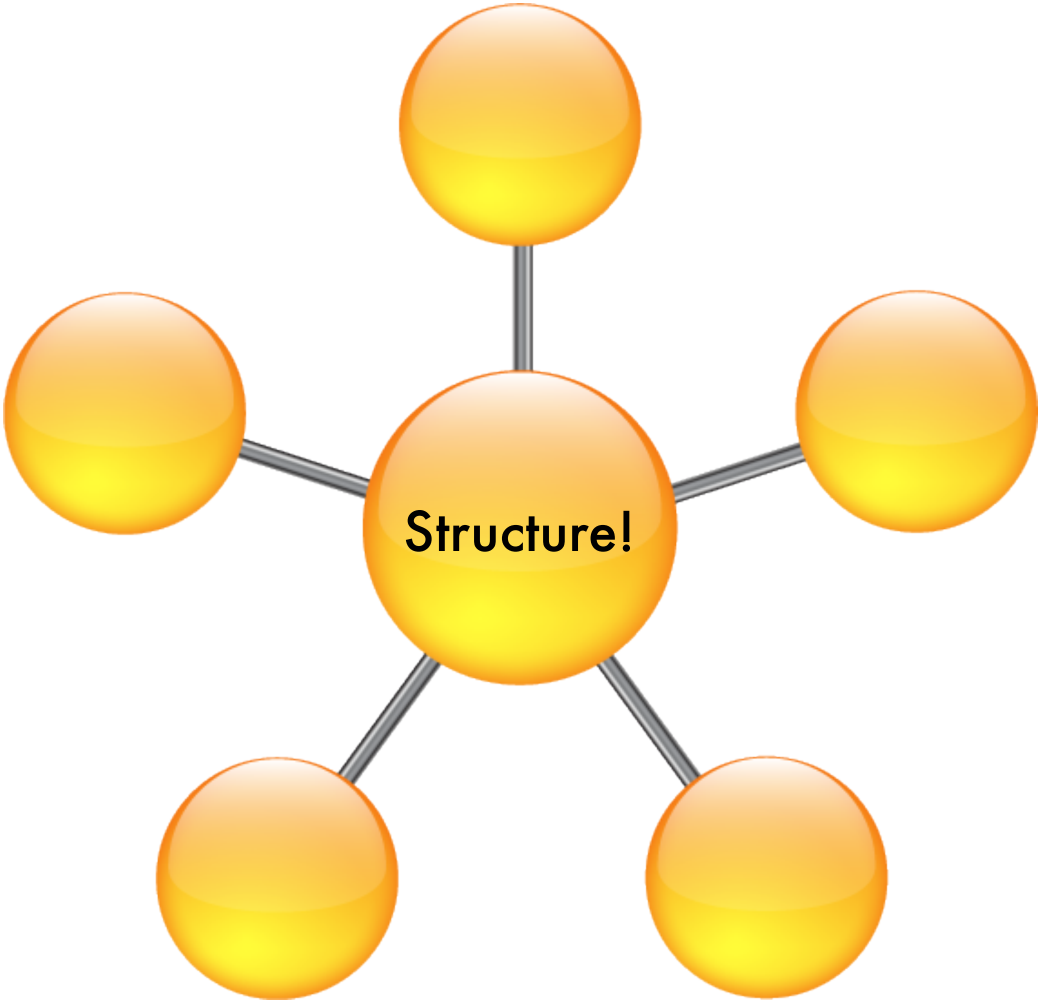
But IGTK!

Why both standards?

What did we want?

- Data!
- Protection from risk
- Prevention of reputational damage
- Ability to support increased collaboration
- Competitive advantage.

What did 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
- A really good selling point!

Bonus!

ISO 20000-1, Service management

ISO 22301:2012, Societal security: Business continuity management systems

ISO 20121:2012, Event sustainability management systems

ISO 9001:2015, General quality management

Common Text

ISO 39001, Road-traffic safety (RTS) management systems

ISO 14001:2015, Environmental management

ISO 55001, Asset management

ISO/IEC 27001:2013, Information technology: Security techniques, Information security management systems

ISO 30301:2011, Information and documentation: Management systems for records

Indicators

- More than one standard
- Standards relate to information security
- Other standard using the Common Text
- Formal reporting requirements
- Sensible scope
- Top level buy-in.

How it worked

Areas of interest

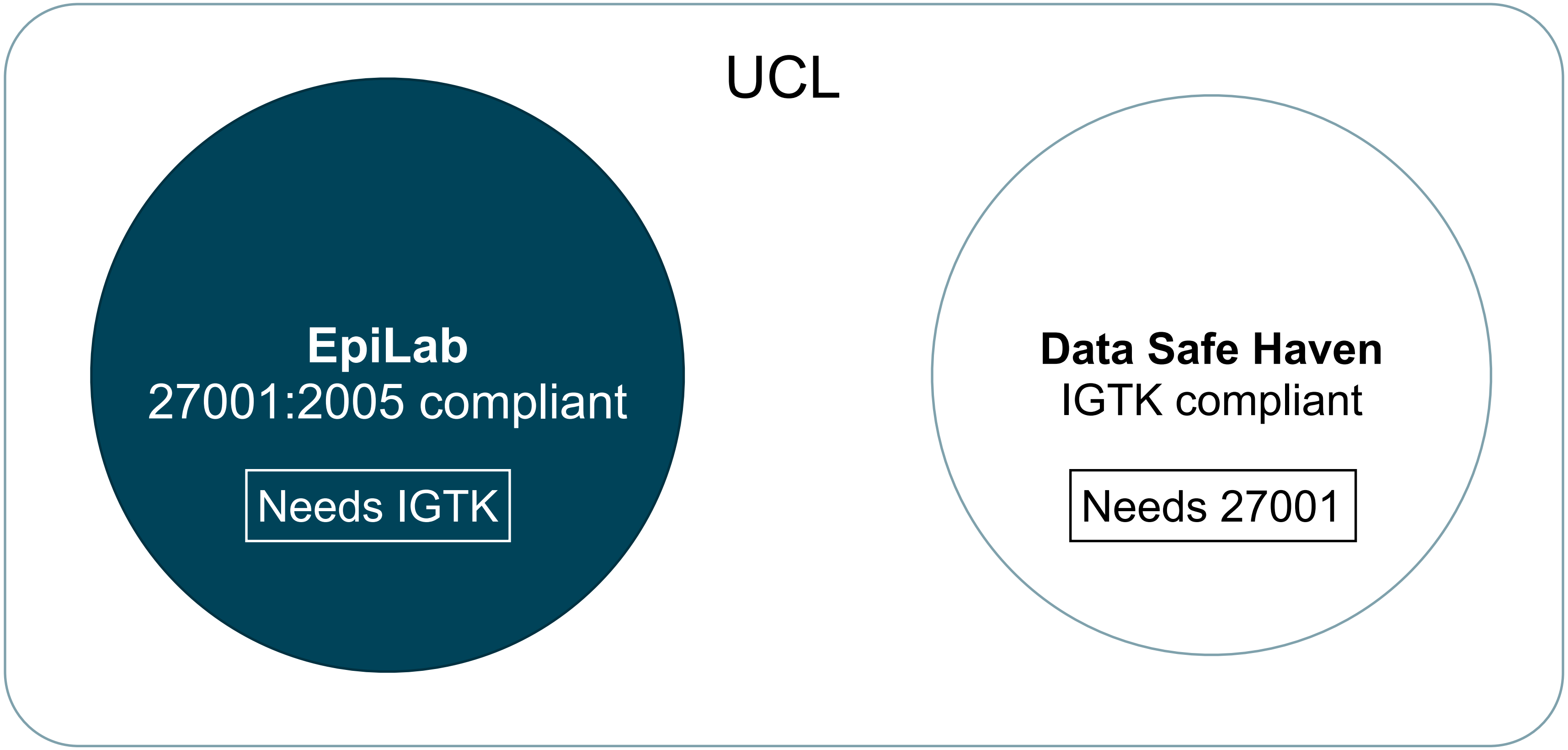
EpiLab

- Small research study
- 27001:2005 compliant
- Outsourced data storage
- Clear scope

IDHS/Data Safe Haven

- Environment for IGTK related data
- Associated governance and support for "customer" studies
- Used by other internal customers
- Designed to be scalable
- UCL hosted

Our situation (early 2013)



UCL

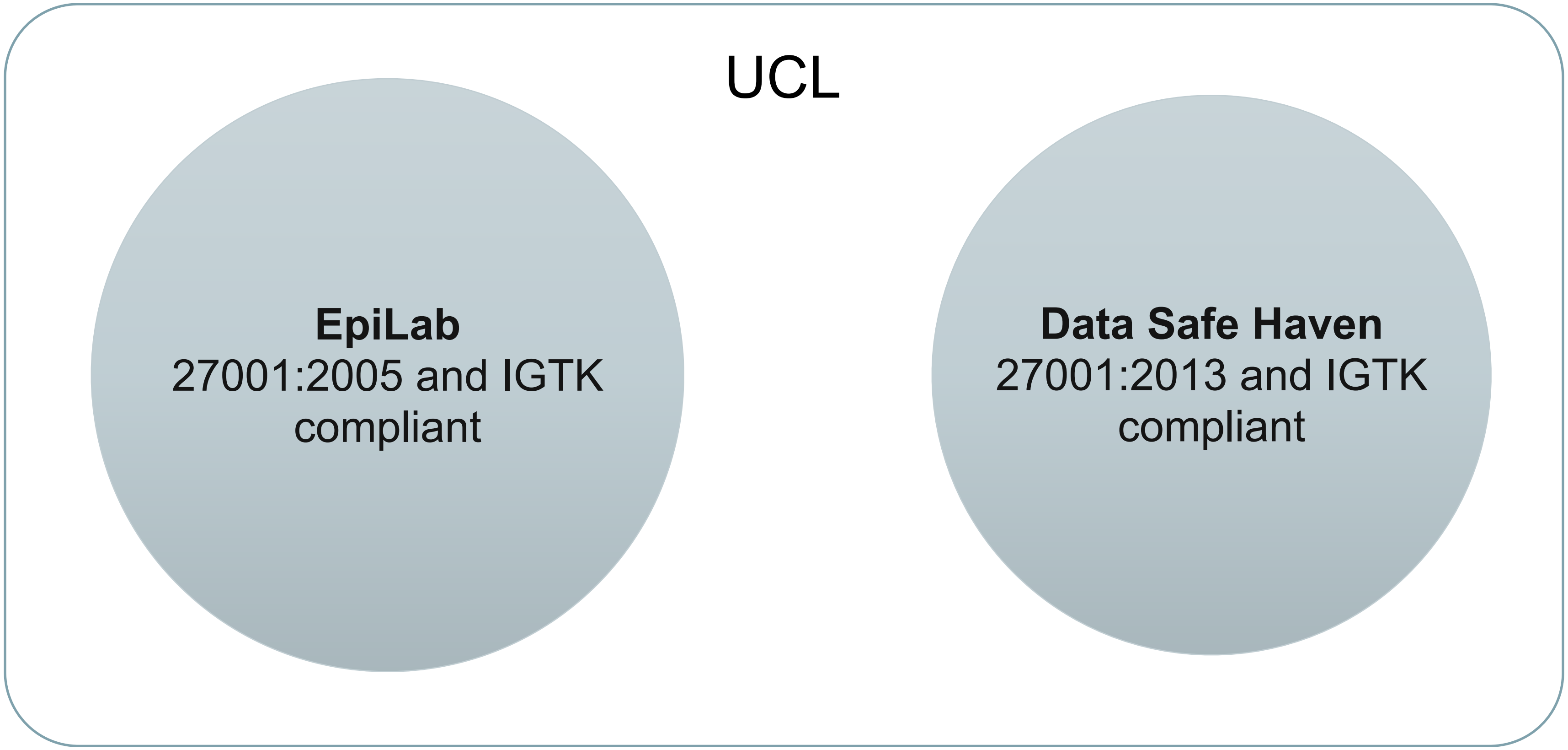
EpiLab
27001:2005 compliant

Needs IGTK

Data Safe Haven
IGTK compliant

Needs 27001

Our decision

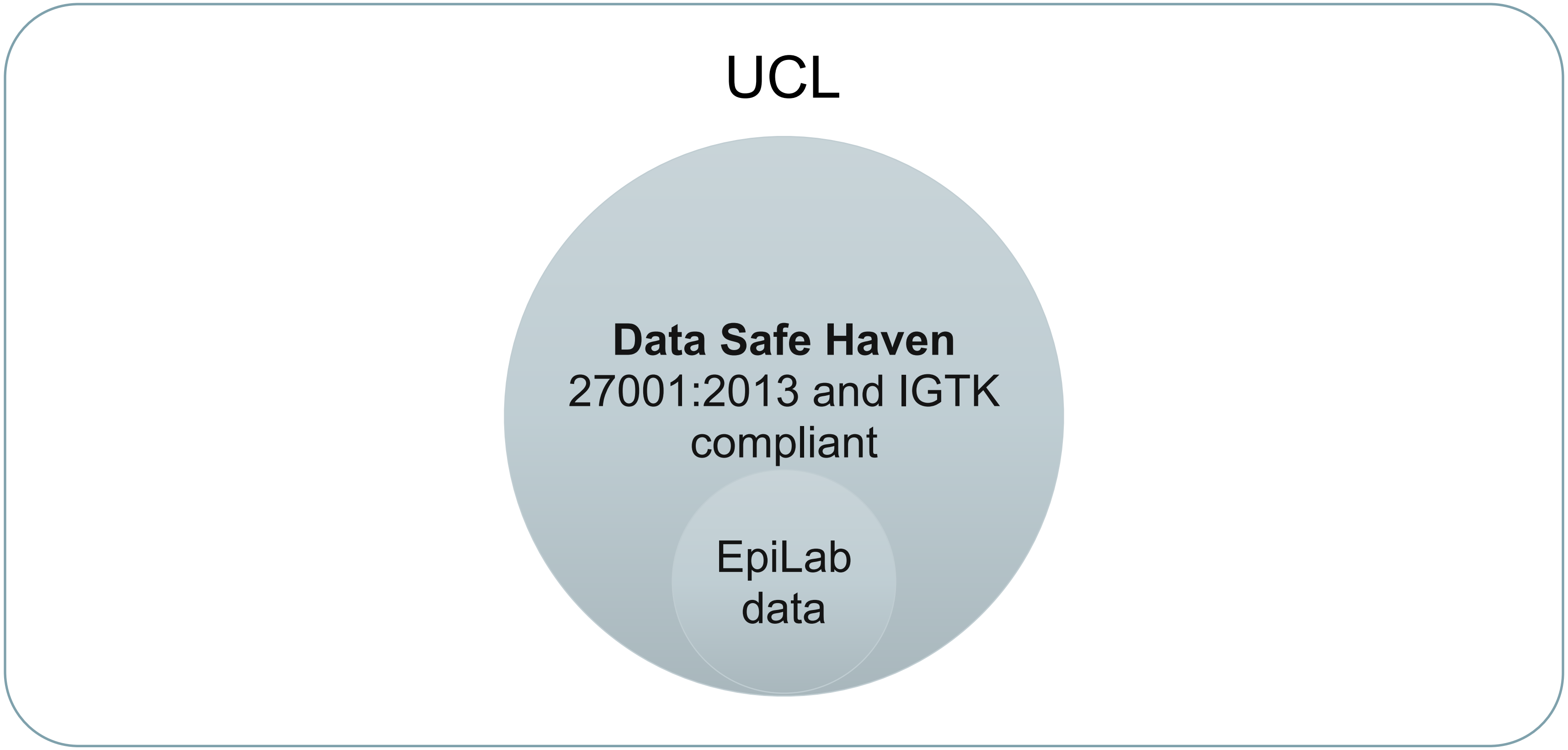


UCL

EpiLab
27001:2005 and IGTK compliant

Data Safe Haven
27001:2013 and IGTK compliant

Next



UCL

Data Safe Haven
27001:2013 and IGTK compliant

EpiLab data

Approach to 27001 adoption

- HSCIC "Information Governance" **is** 27001 "Information Security"
- Part of Data Safe Haven project
- Treat IGT as externally defined requirements (C4)
- Used external consultant
- Close collaboration with central information security
  - Linked management structure
  - Acting as internal audit
- Meetings weekly.

Standard risk list

- Spam
- Phishing
- Brute force
- Malware

Hacking

- Denial of service
- Misuse
- User damages info
- User leaks info
- Theft/loss of mobile devices
- Theft/loss of non-mobile devices
- Theft/loss of paper based info
- Software failure
- Power failure
- Internet/comms failure
- Hardware failure
- Premises break-in
- Act of God, vandals, terrorists

The audit- May 2014

- Two stages:
  - Stage 1 to verify paperwork
  - Stage 2 to test ISMS functionality
- Expect auditor to ask for evidence at Stage 2
- Risk treatment plan should match risk assessment
  - No controls implemented without being in risk treatment plan
  - Expect almost all controls to be relevant
  - What if you have to accept an intolerable risk?

Progress

- EpiLab compliant with IGTK (took 3 months)
- Data Safe Haven recommended for 27001 certification (took 1 year).

Assembling the evidence

- Carried out gap analysis
- Governance already in place
- Policies generally already done
- Training already in place for customers
- Combined multiple duplicate processes
- Most necessary controls already implemented
- Used risk assessment to connect dots with controls already implemented.

Additional security measures

- Reviewing access rights regularly:
  - Research staff
  - Support staff
- Training needed for support staff
- Checking bins for paper data
- Internal audit of every part of the standard over a three year period.

Tips

Things to bear in mind

- Get some training
- Consider professional assistance
- Short scope statement
- Reverse engineer
- Control is NOT irrelevant if actually in place!
- Internal audit- and compliance- should be ongoing
- External audit is a constructive experience
- Scope is very challenging
- Raises awareness.

Should you certify?

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

Most importantly...

- YOU ALREADY HAVE AN ISMS!

Thanks for listening!
Any questions?