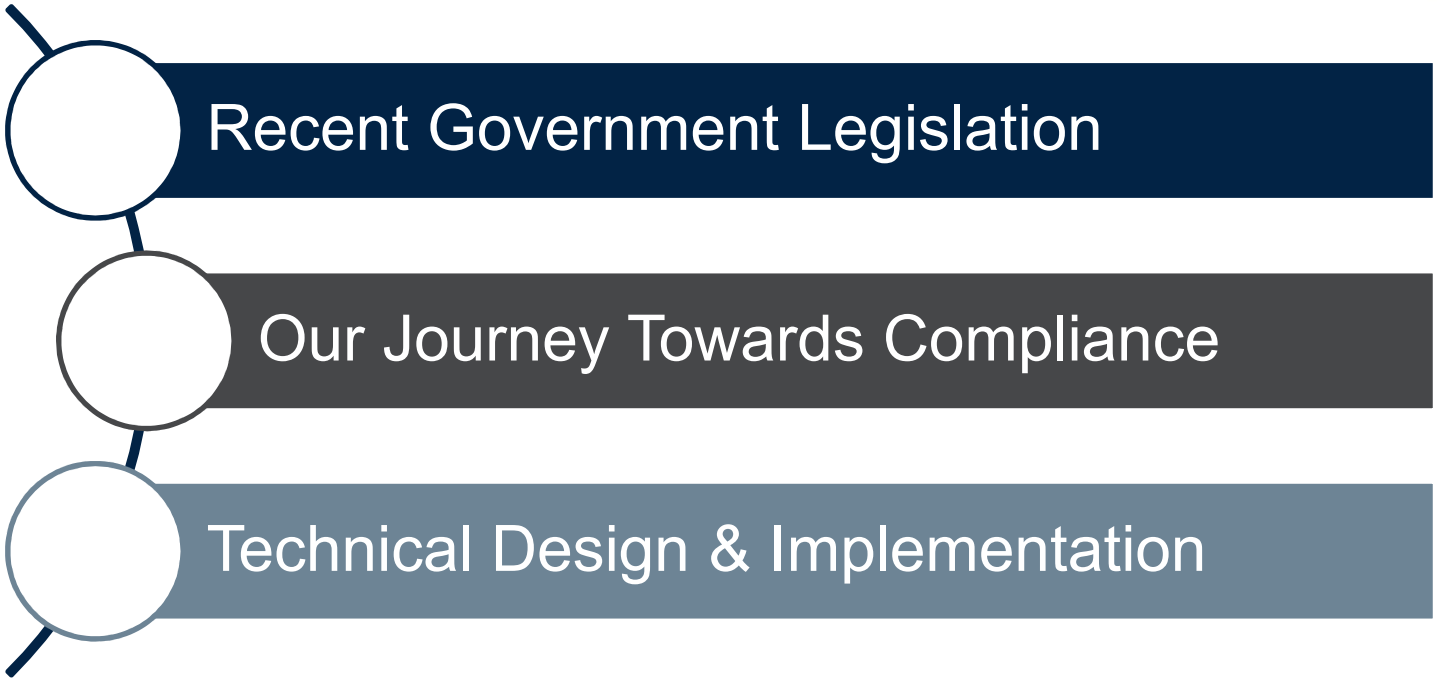
Technically, this is what Federal Legislation looks like!

The Road to Technical Compliance

Peter Vanheck & Simon Coggins
QUESTnet 2018 Conference, Cairns.

What is this presentation about?



Recent Government Legislation

Our Journey Towards Compliance

Technical Design & Implementation

1. Notifiable Data Breaches

An eligible data breach is where a ***reasonable person*** would conclude that there is a likely ***risk of serious harm*** to any of the affected individuals as a result of unauthorised access or disclosure.

** Privacy Act 1988, Privacy Amendment (Notifiable Data Breaches) Bill 2016*

2. Data Retention

Service providers are required to retain and secure for two years, specific telecommunications data relating to the services they offer.

** Telecommunications Act 1997, (Interception and Access) Amendment (Data Retention) Bill 2015*

Recent Government Legislation

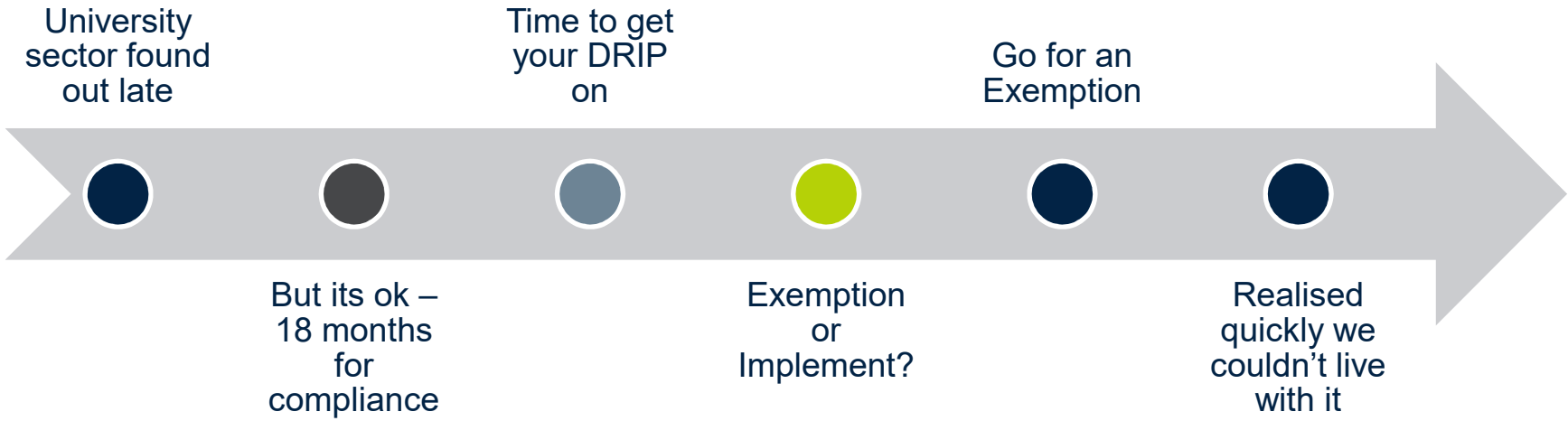
Our Journey Towards Compliance

Technical Design & Implementation

Our Journey: Notifiable Data Retention


Winding

It was a bumpy ride!

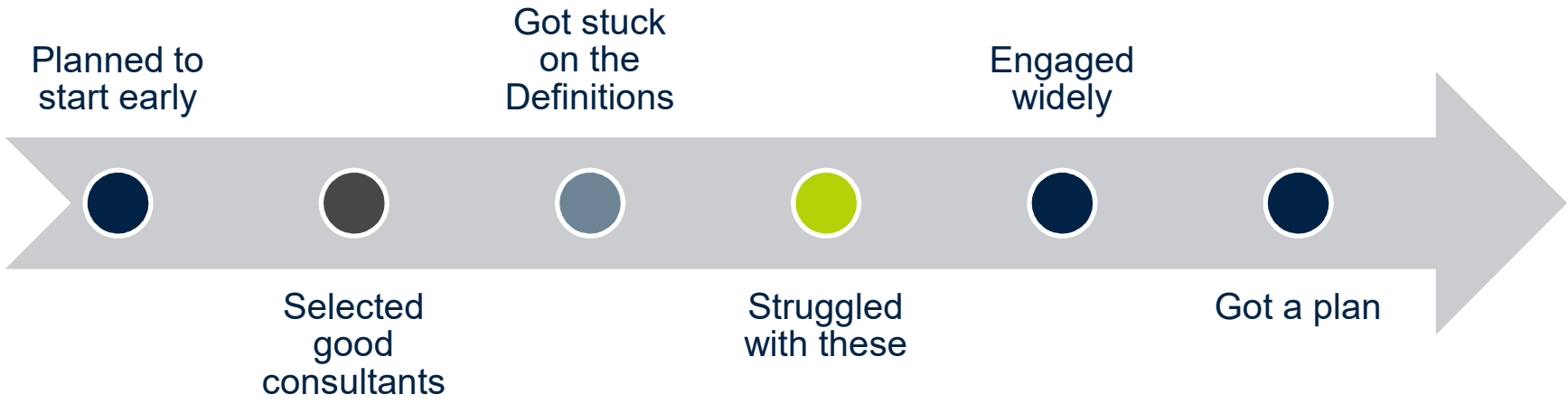


https://www.downergroup.com/httpswwwdownergroupcomnews , viewed Sept 2018.

Our Journey:
Data Breaches


Smooth

A much smoother ride!



Definitions: Data Breaches

What is a reasonable person?

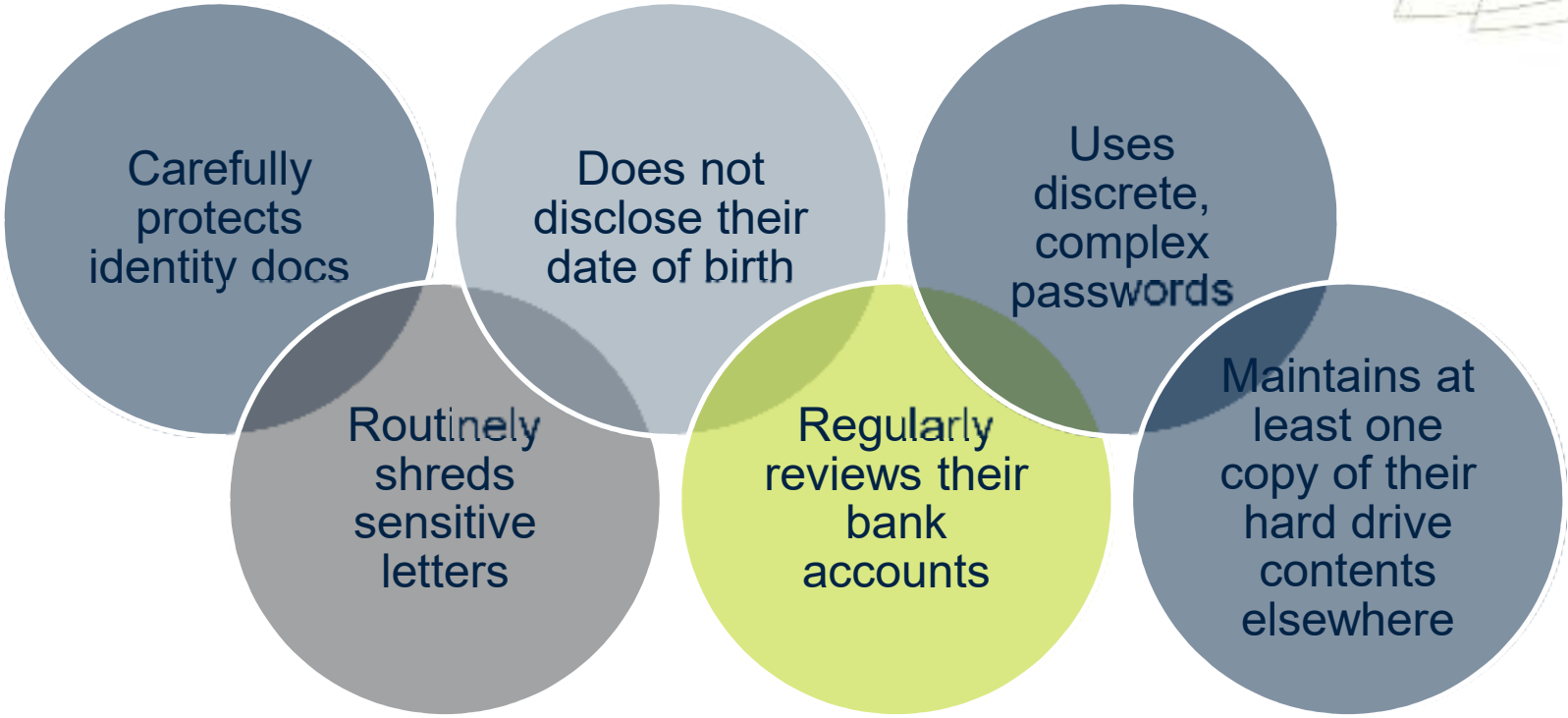
What is serious harm?

1. Notifiable Data Breaches

An eligible data breach is where a *reasonable person* would conclude that there is a likely *risk of serious harm* to any of the affected individuals as a result of unauthorised access or disclosure.

** Privacy Act 1988, Privacy Amendment (Notifiable Data Breaches) Bill 2016*

A Reasonable Person ….



Serious harm means ….

Category	Key Questions
Identity theft	• Will use of the personal information provide the ability to open bank accounts, establish phone or data (fixed/mobile) services or access government services? • Will the use of personal information enable the identity to be impersonated, enabling access to information that will provide the ability to open bank accounts, establish phone or data (fixed/mobile) services or access government services?
Financial loss	• Will the use of the personal information provide the ability to access any other monetary products? • Will the use / disclosure of the personal information lead to financial losses?
Threat to physical safety	• Will disclosure of the personal information reveal an individual's identity or location that would not otherwise be known?
Threat to emotional wellbeing OR humiliation and damage to reputation or relationships	• Will the disclosure of personal information disclose details of sensitive medical conditions? • Will the disclosure of personal information disclose relationship issues that would not otherwise be known? • Will the disclosure of personal information disclose details of legal proceedings that would not otherwise be known?
Loss of business or employment opportunities	Will disclosure of the personal information directly limit their employment or business opportunities?
Workplace or social bullying or marginalisation	Will disclosure of the personal information limit the individual's social activities?

Other	• Will any of the following possible harms be realised?
	  • the loss of public trust in the agency, government program, or organisation
	  • reputational damage
	  • loss of assets (e.g., stolen computers or storage devices)
	  • financial exposure (e.g., if bank account or credit card details are compromised)
	  • regulatory penalties (e.g., for breaches of the Privacy Act)
	  • extortion
	  • legal liability, and
	  • breach of secrecy provisions in applicable legislation

Recent Government Legislation

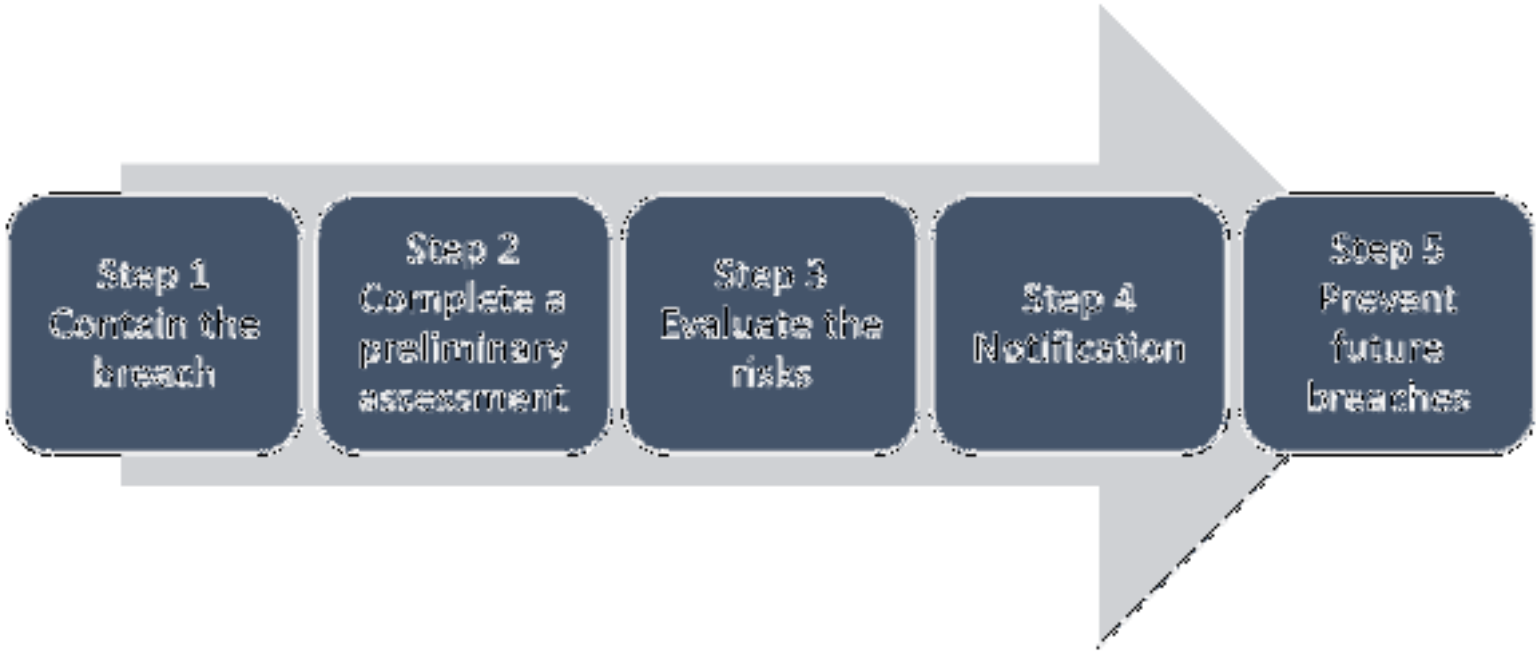
Our Journey Towards Compliance

Technical Design & Implementation

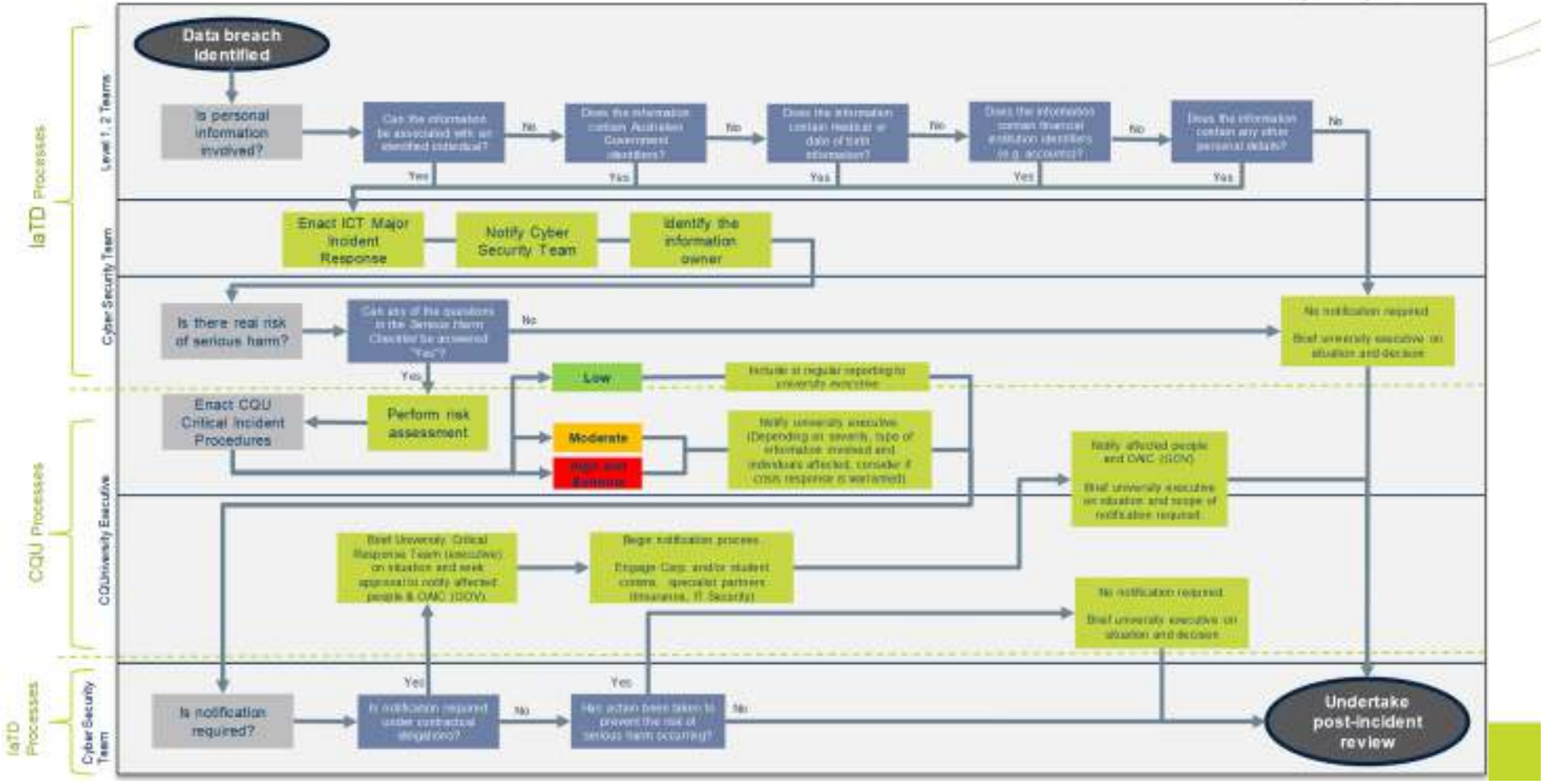
Notifiable Data Breaches

Process Flowcharts

High Level Process



Response Process Flowchart



Challenges

Definitions

- What was a reasonable person?
- What serious harm meant?

CQU's Critical Response Team

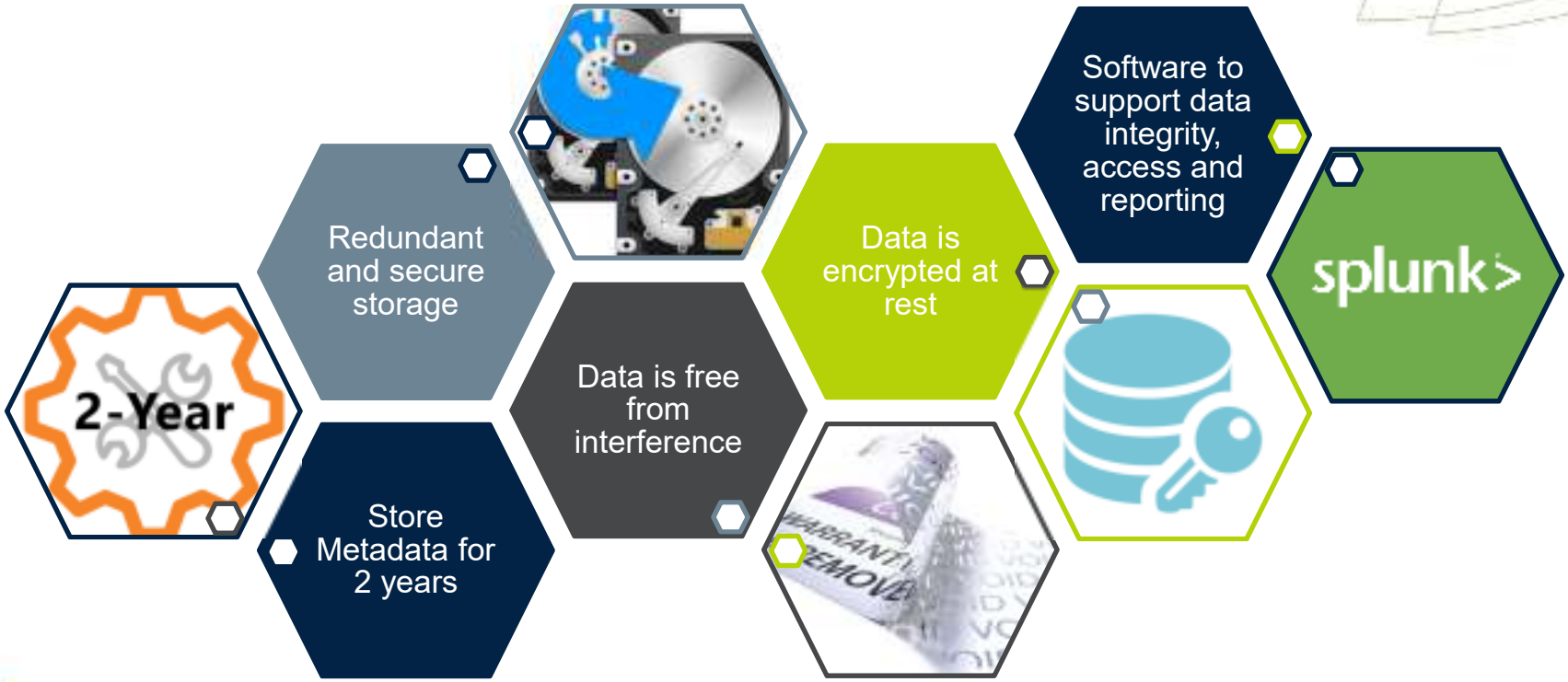
- Getting recommendations back quickly

4-7 Day turnaround

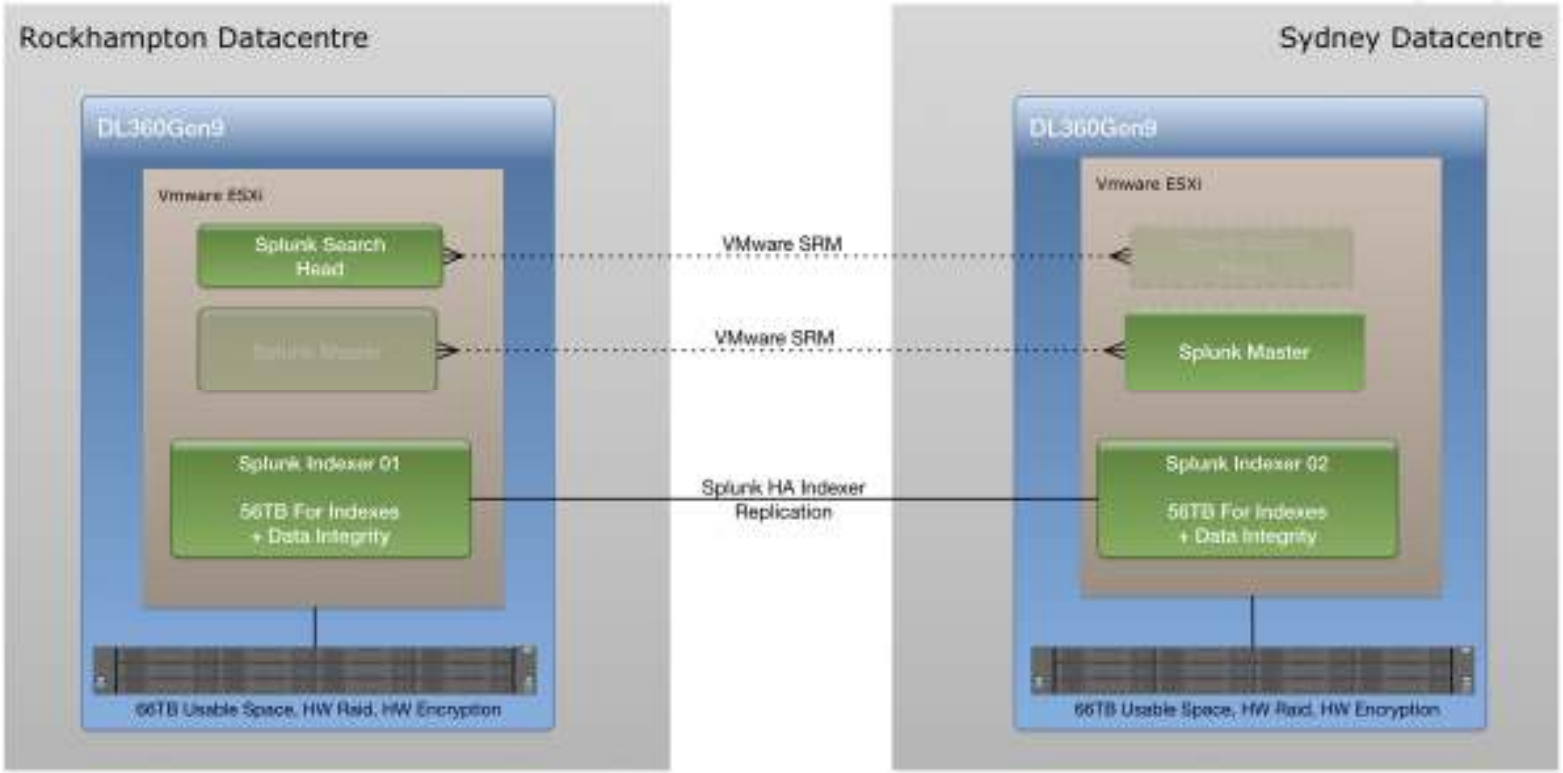
Data Retention

Technical Overview with Simon Coggins

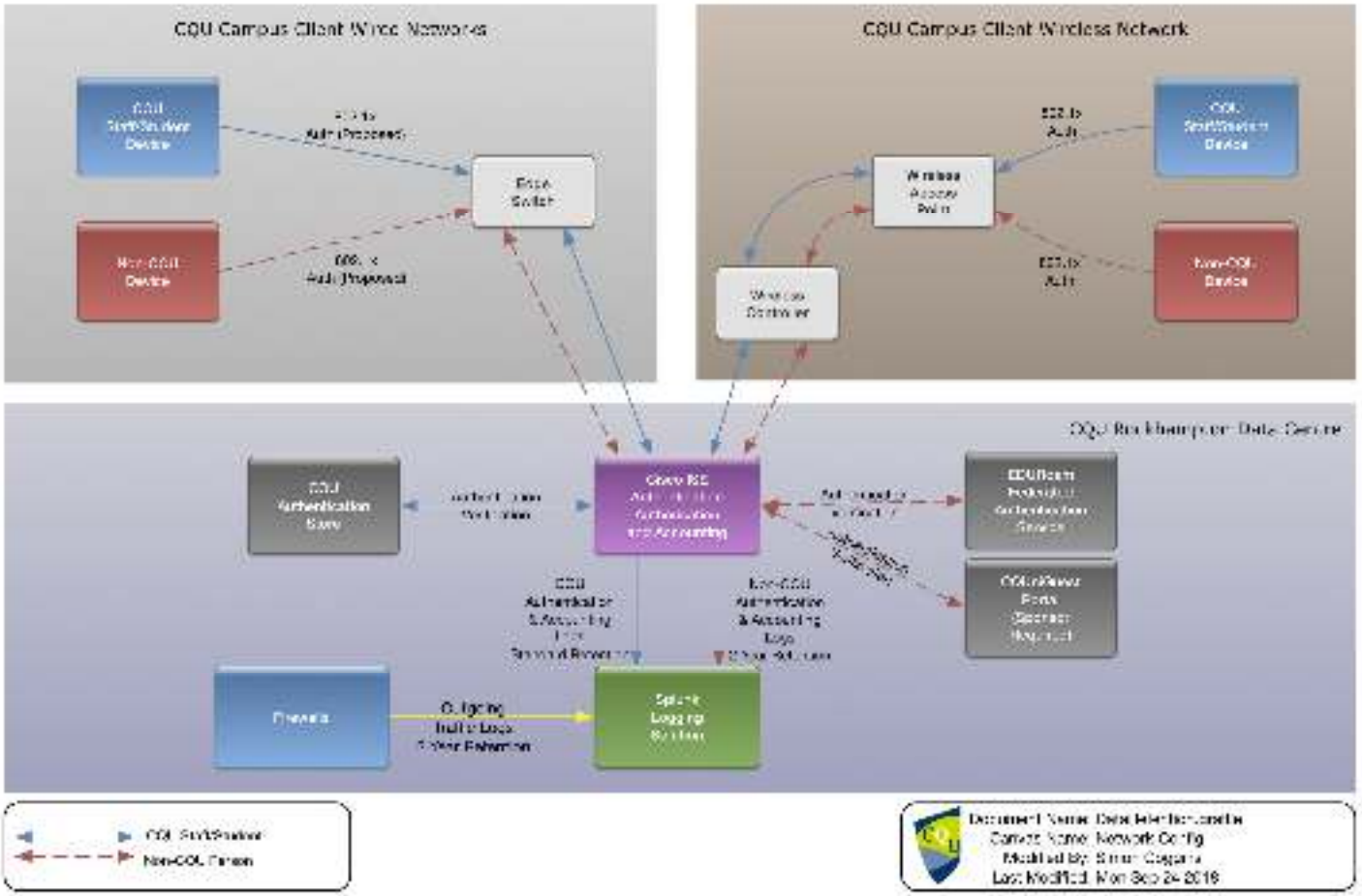
Design Criteria



Splunk HA Architecture



Network Architecture



Challenges

No existing vendor solutions, DIY solution required.

External/Generic Accounts

- Singapore Army
- Academics sharing Wi-Fi logins
- Visiting Students from Schools
- Conference delegates / eduroam users

Law was written for telecom, with an internet band aide