FUJITSU

shaping tomorrow with you

An Interpretation of the new Government Security Classification Scheme

26th March 2014

SECURE THINKING

Today's presenters

- **Tom Roche**
  Head of Public Sector
  Fujitsu UKI

- **David Robinson, MBE**
  Chief Security Officer
  Fujitsu UKI

- **John Alcock**
  Head of Security Professional Services
  Fujitsu UKI

Health Warning

This webinar represents a Fujitsu UK&I understanding of the new Government Security Classification Scheme.

It is an interpretation of the content of various briefings and of material released by HMG.

The new scheme will develop and further material will be released over the coming months so please refer to a suitably qualified security specialist for up-to-date information.

The Old Scheme

Protective Marking

- A label that denotes the measures that need to be taken to maintain the confidentiality of a piece of information.
- These measures are in the areas of physical, personnel, procedural and technical controls.

You can derive a relationship from a protective marking to an Impact Level - but it is definitely not safe to do so the other way.

Business Impact Level

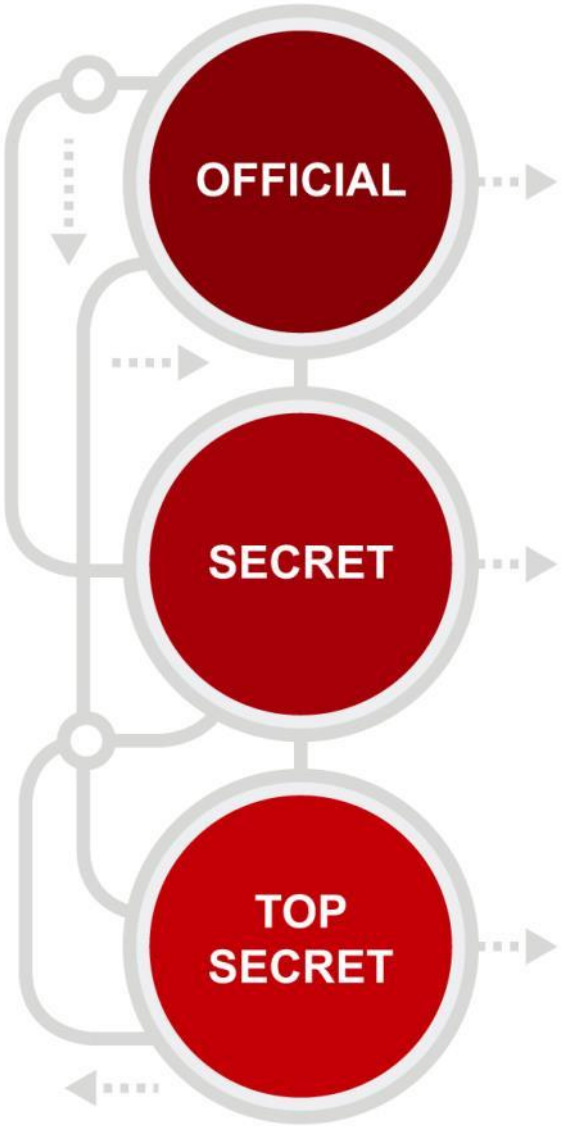
- A means to express the consequences of a piece of information being compromised on a scale of 1-6.
- Compromise could affect the information's confidentiality, integrity or availability and impact is likely to be different in each criteria.
- Business Impact Levels have been useful in modelling risks and understanding the implications of a threat being realised.

The New Scheme

- Why?
  - To enable reform
    - Contribute to a “far better experience at lower cost”
    - Protected by default
    - Maintain principles of risk assessment
  - Change is a good thing to shake-up an organisation.

- Policy is complete and has been released
- Launched October 2013 with “Go Live” set for 2nd April
- “Departments going great guns”.
- Cabinet Office has explained that “go live” was just a milestone on a transition journey.

The Three Tiers

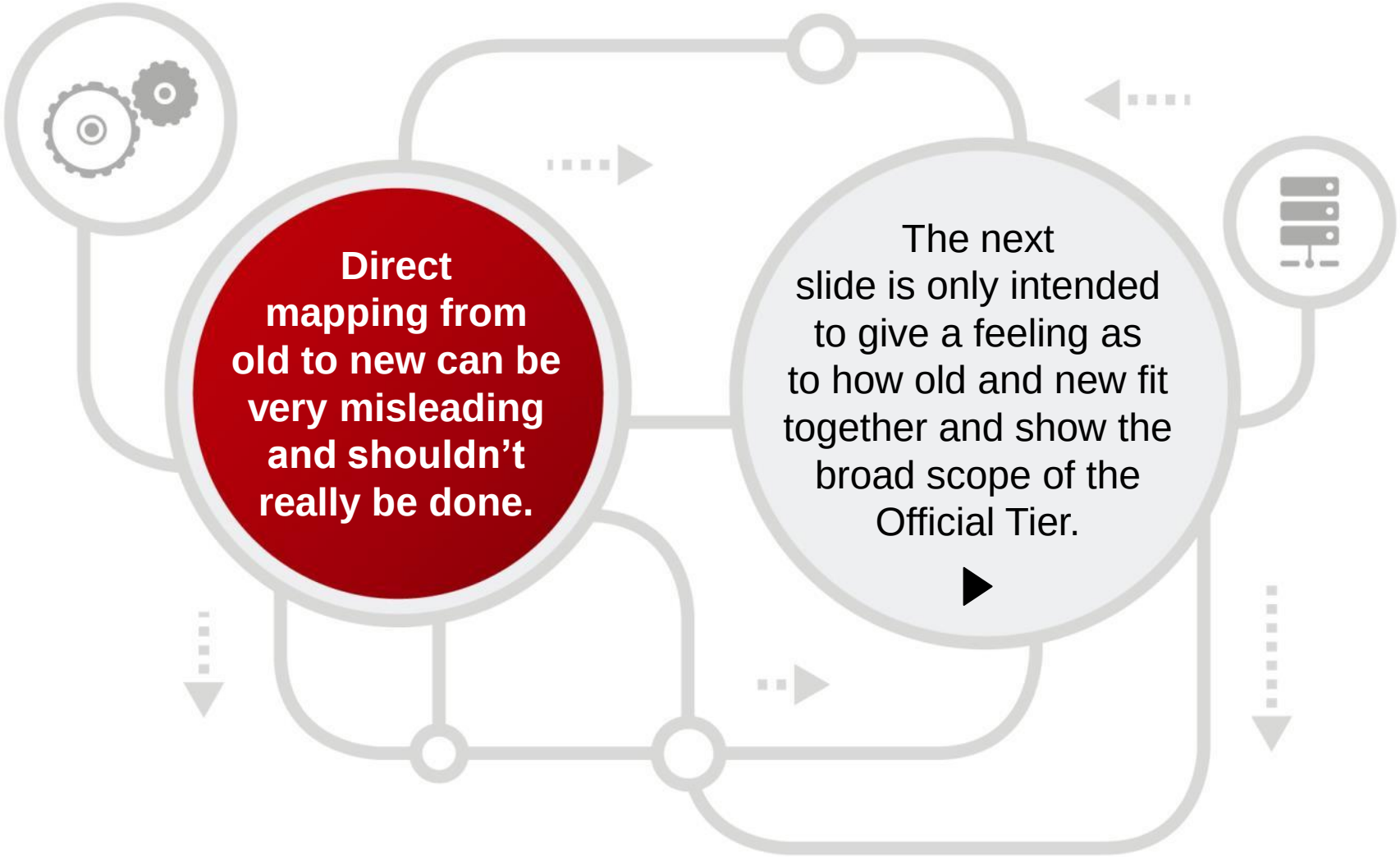


- **All routine public sector business;** potentially including policy development, service delivery, legal advice, personal data, contracts, statistics, case files, and administrative data.

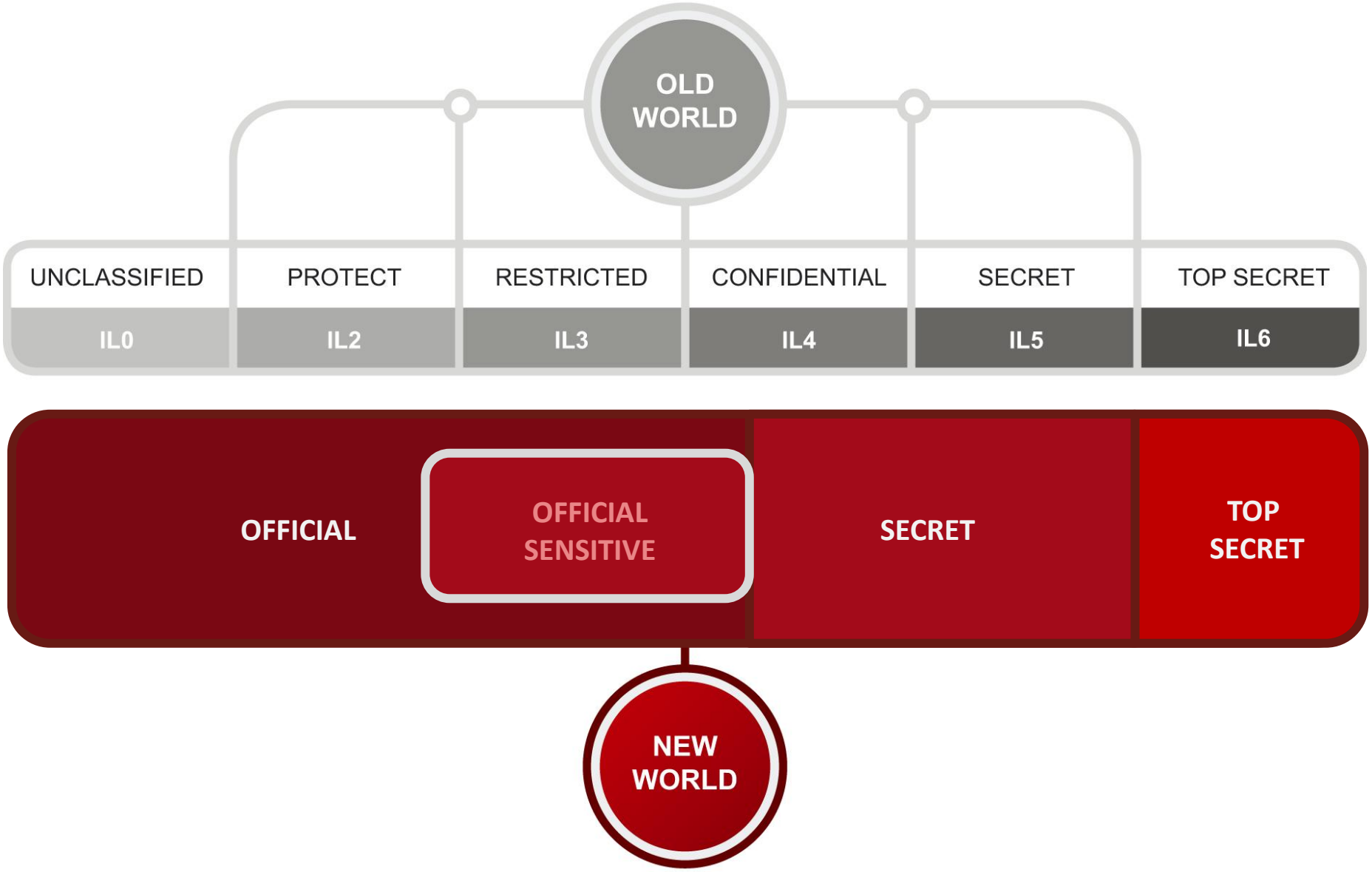
- **More sensitive defence, diplomatic, information or** security assets that must be protected against heightened threat conditions (i.e. targeted attack from sophisticated and determined threat actors) ***and where*** *the impact of compromise is significant.*

- **Exceptionally sensitive** assets that directly support or threaten the National Security of the UK and our allies and require extremely high protection from all threat sources.

Health Warning



The New World



The Official Tier

In outline:

- OFFICIAL information must be secured against a threat model broadly similar to that faced by a large UK private company.
- Defend data and services against compromise by attackers with bounded capabilities and resources.
- These controls will provide robust and effective protection that make it very difficult, time consuming and expensive to illegally access OFFICIAL information.

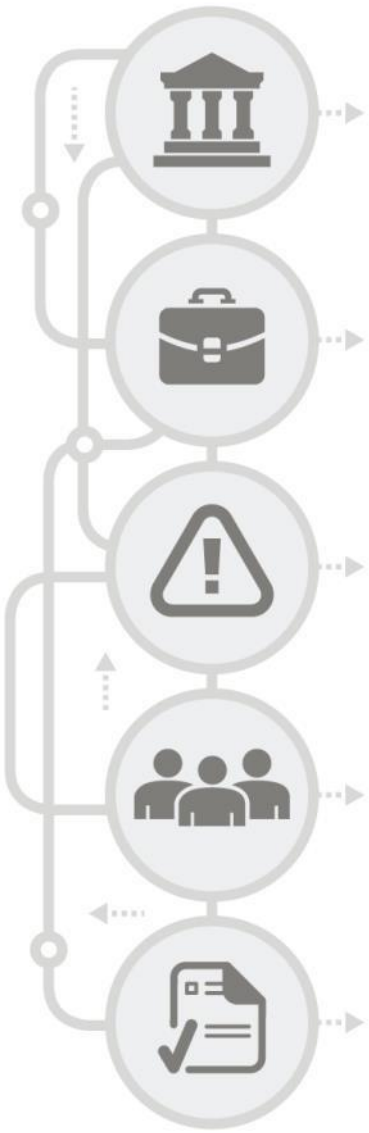
Which means:

- A move away from being label monkeys.
- Choosing the right security for the organisation's environment.
- A strong emphasis on best practice.
- No need to apply markings.
- A greater emphasis on departments to specify requirements correctly.

The Official Tier

Within the OFFICIAL tier there will be a range of information with varying degrees of business impact, should the risks be realised.

Risk Management and Impact Levels



- Public Sector organisations own and manage their own information risk, within the bounds of a top level HMG risk appetite set by the SCaRAB (Senior Cyber and Risk Assurance Board).
- Cabinet Office & CESG want HMG to manage risks effectively.
- Business Impact Levels dominate risk management but are misused and in many ways ‘wedded’ to the outgoing GPMS.
- The Policy Implementation Board has asked CESG to reform how impact assessment is undertaken.

Current Position and Challenges

- There is a transitional arrangement in place for the old CONFIDENTIAL.
- There is concern over the timing of the release of the next tranche of documentation from CESG.
- We know that aggregated data sets should be considered to be within the same classification level but there is no case law yet.
- Suppliers don't yet understand how to handle OFFICIAL on their corporate systems.
- No immediate changes are being made to IT systems to reflect the demise of RESTRICTED, PROTECT and UNCLASSIFIED.
- Departments need to understand their information, the risks that they're exposed to and the way their partners are embracing the changes.
- Stop labelling and think in terms of business and security requirements.

The new scheme in practice for the Cloud

Assured Public Cloud (formerly Impact Level 2, 2, x) services will be subject to a suitably scoped ISO27001 certification and other assurance activities as described in the *GCloud Information Assurance Requirements and Guidance.*

- Such services may be appropriate for the generality of OFFICIAL information, although organisations should carefully consider the scope of the IS027001 certification, the geographic location of the hosting, and any other residual risks identified as part of the G-Cloud Accreditation Statement. It is unlikely that these services will be suitable for more sensitive information.

Formally accredited Public Cloud (formerly Impact Level 3, 3, x) or Private Cloud services will be subject to a full HMG accreditation and will be hosted within the UK.

- These services are likely to be appropriate for most OFFICIAL information, although organisations should still be mindful of any risks involved in outsourcing services and data to the cloud.

How we secure our customers

Professional Services

Unparalleled Skills & Experience

Take advantage of our experts from Information Assurance (CLAS) to Technical Design, Implementation, and Continuity.

Products

Strong OEM Relationships

Long standing vendor relationships to provide our customers with fit for purpose, best of breed technology.

Managed Services

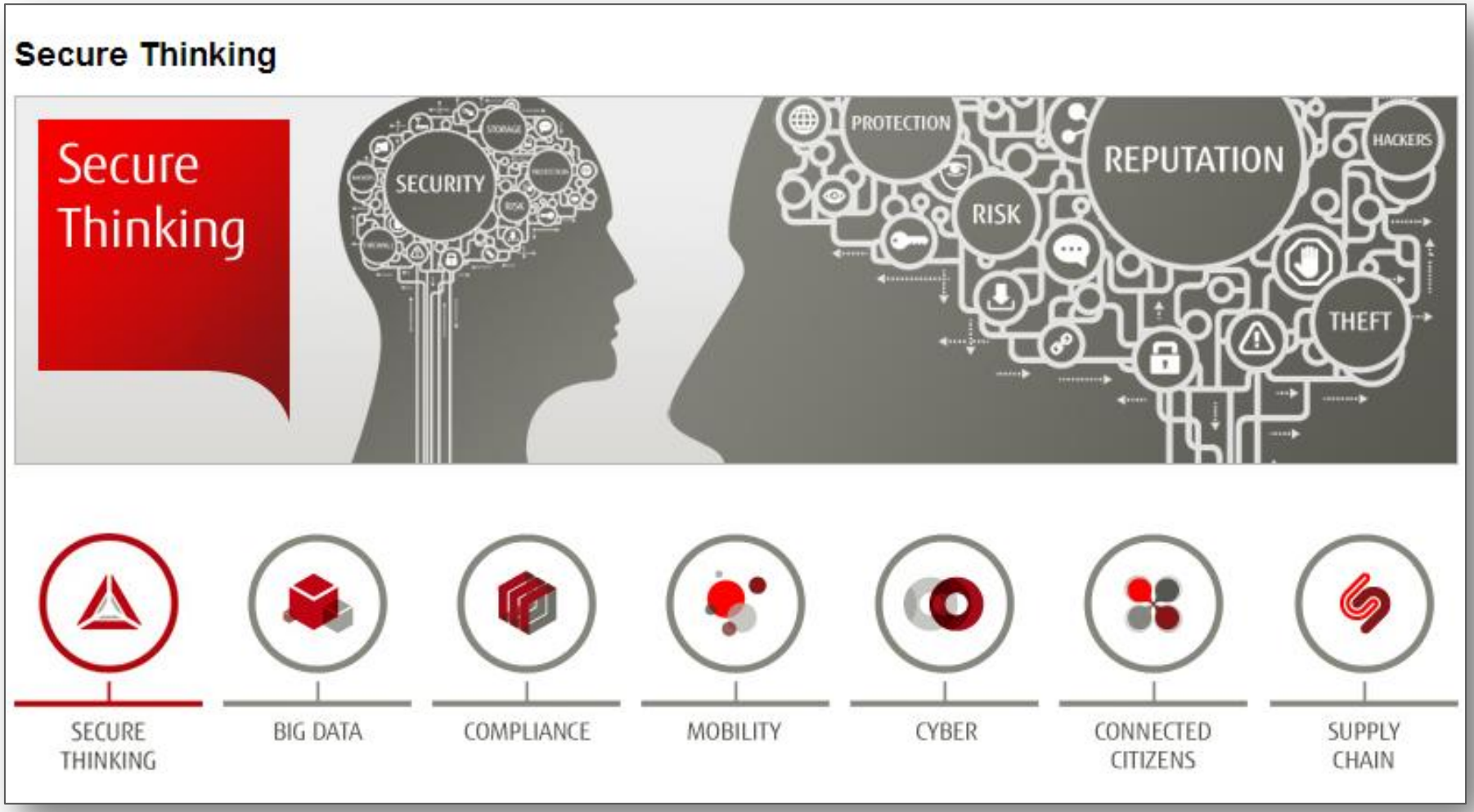
Keeping You Secure, 24x7x365

Advanced security operations keep our customers secure, with service levels to meet any requirement from adhoc support to fully managed.

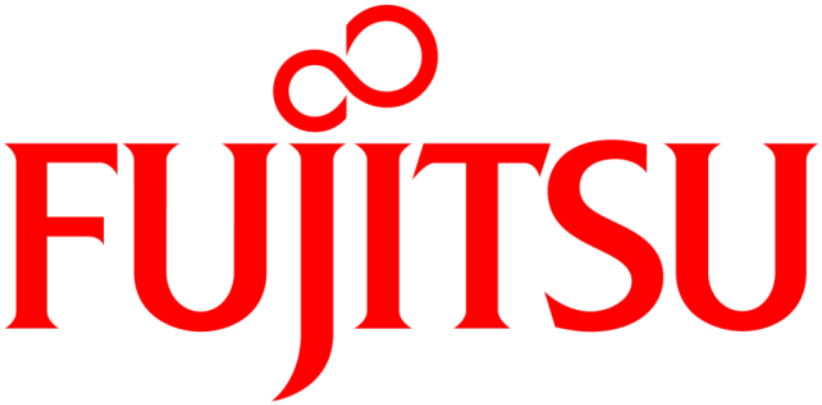
Further resources

https://www.gov.uk/government/publications/security-policy-framework

For more information



http://www.fujitsu.com/uk/campaigns/secure-thinking/index.html



shaping tomorrow with you