# Fraud and Error in the Social Security System

## Risk Profiling

Session 7, UK

Christopher Jennings, UK Department for Work and Pensions

**WORKSHOP ON**
**REDUCING ERROR, FRAUD & CORRUPTION (EFC) IN SOCIAL PROTECTION PROGRAMS**
**June 8-12, 2014, Opatija, Croatia**

THE WORLD BANK
IBRD • IDA | WORLD BANK GROUP

# Risk Profiling – Why ?

- Recognise that to most effectively tackle fraud and error we need to understand our claimant base, the risks inherent in particular benefits, the risks associated with claimant types and the costs involved in each

- Links not just to individuals but to benefits – e.g. spend in Income Support is relatively low so interventions may not be so cost effective as in other benefits

- Opportunities offered by increased digitilisation, automation and data sharing

# Risk Profiling – Approach

What do we consider ?

- Benefit type
- Transaction type
- Claimant type
- Point of time in claim lifecycle (e.g. child reaching school leaving age)

Information sources:

- Benefit data
- Data from Other Government Departments and public bodies
- Behavioural analysis

# Risk Profiling – Approach

Current use focused on customer types to:

- Target interventions / case cleansing activity
- Prompt campaigns
- Determine cost effective route for investigations

Future use:

- As above
- Risk scoring – how we deal with a claimant from the outset
- Establishing ‘trust’
- Identifying organised criminal activity

# Risk Profiling – Current Activity

- Introducing Risk Based Intervention Criteria to route fraud and error referrals appropriately:

  - national standardised approach based on severity of allegation;

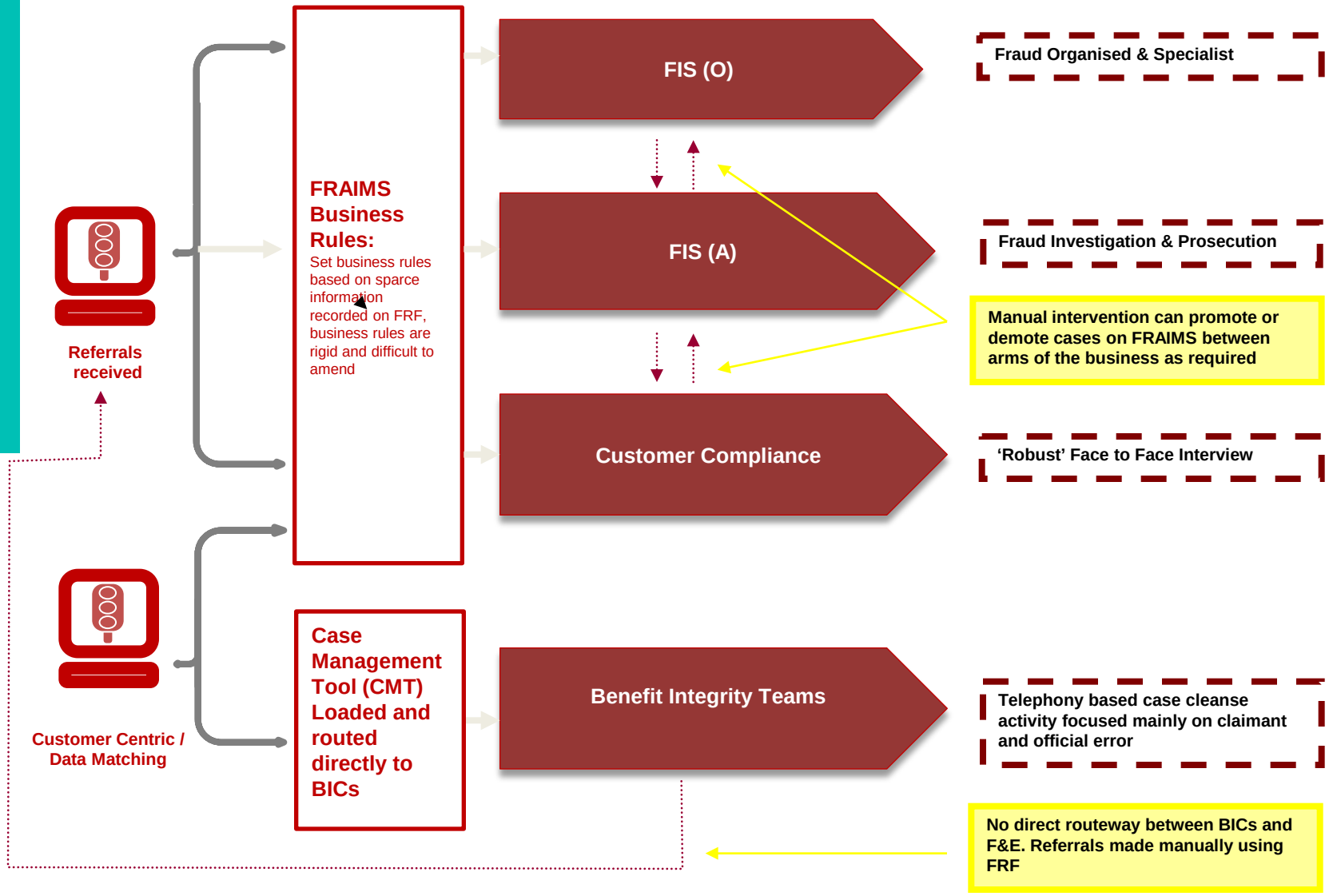
  - flexibility to adjust thresholds in line with current threats and our response capability.

- Allows for additional options around punishment and cost effective treatment of offenders

- Allows greater volume of cases to be dealt with without face-to-face interventions

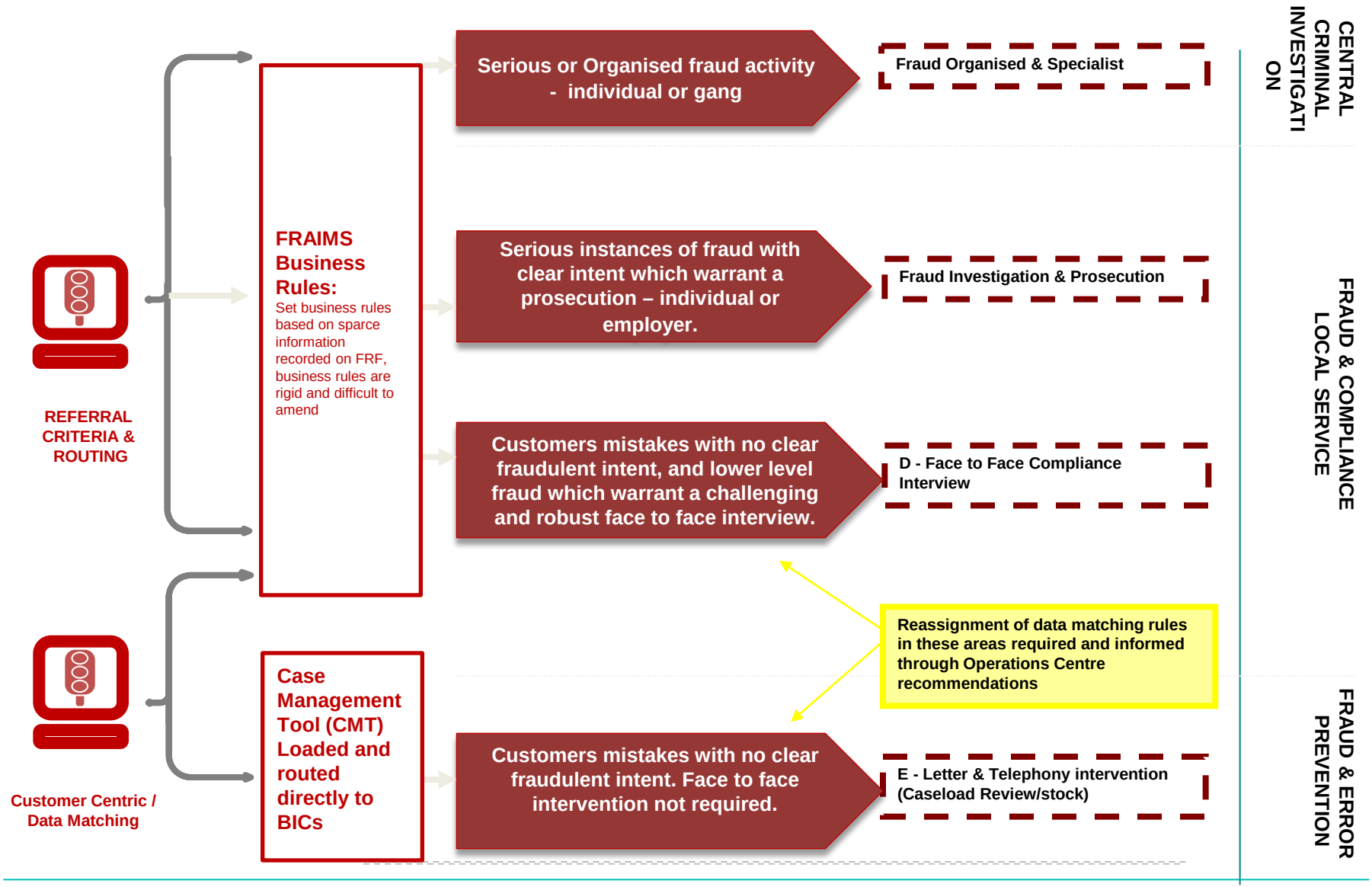
# F&E Service: Risk Based Intervention Criteria overview.

## Pre-April 2014



# F&E Service: Risk Based Intervention Criteria overview.

## Post April 2014



# F&E Service: Risk Based Intervention Criteria overview

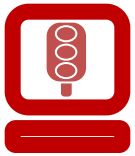
## Future view

**F&E INTERVENTION RANGE – April 2014**

Those highlighted in dashed red are available from 2014

**Cyber Desk**

**Cyber threats**



**REFERRAL CRITERIA & ROUTING**

**Risk & Intervention Rules:**

Govt./Dept Priorities
Risk Appetite/threshold
Value of potential loss & VfM
Customer group

**Serious or Organised fraud activity - individual or gang**

**A - Fraud Organised & Specialist**

**Serious instances of fraud with clear intent which warrant a prosecution – individual or employer.**

**B - Fraud Investigation & Prosecution**

**Less serious instances of fraud with clear intent which warrant a 'penalty'**

**C – THRESHOLD FRAUD**

**This is a new area requiring development**

**Customers mistakes with no clear fraudulent intent, which warrant a challenging and robust face to face interview.**

**D - Face to Face Compliance Interview**

**Customers mistakes with no clear fraudulent intent. Face to face intervention not required.**

**E - Letter & Telephony intervention (Caseload Review/stock)**

**CENTRAL CRIMINAL INVESTIGATION**

**FRAUD & COMPLIANCE LOCAL SERVICE**

**FRAUD & ERROR PREVENTION**

*Note: Official Error cases follow a different routing process which is not shown on this slide*

# Risk Profiling – the Future

- Developing an Analysis and Intelligence Hub to support Universal Credit
- High security accreditation with access to information held across Government, including Government Communications Headquarters
- Hub will develop risk profiles for customers, transactions and 3rd parties at both onset and throughout the life of a claim
- Hub will prompt appropriate intervention to nudge claimants into compliance, to support a proportionate verification strategy and identify and expose organised / systemic fraud
- Aspiration is to automate these process and support digital delivery across the range of benefits

# Lessons Learned

- Still learning ! Plenty going on across Government – learning lessons from other leaders in field
- Still in early days of digital delivery – risk profiling both informs design and delivery of these services
- Importance of skilled staff with best intelligence – may mean investment in training, security and processes
- Must be reactive to needs of the business
- Processes have to be responsive
- Evaluation