

# **IT & Data Security and the FSA**

## **22<sup>nd</sup> April 2010**

**Jill Savager**

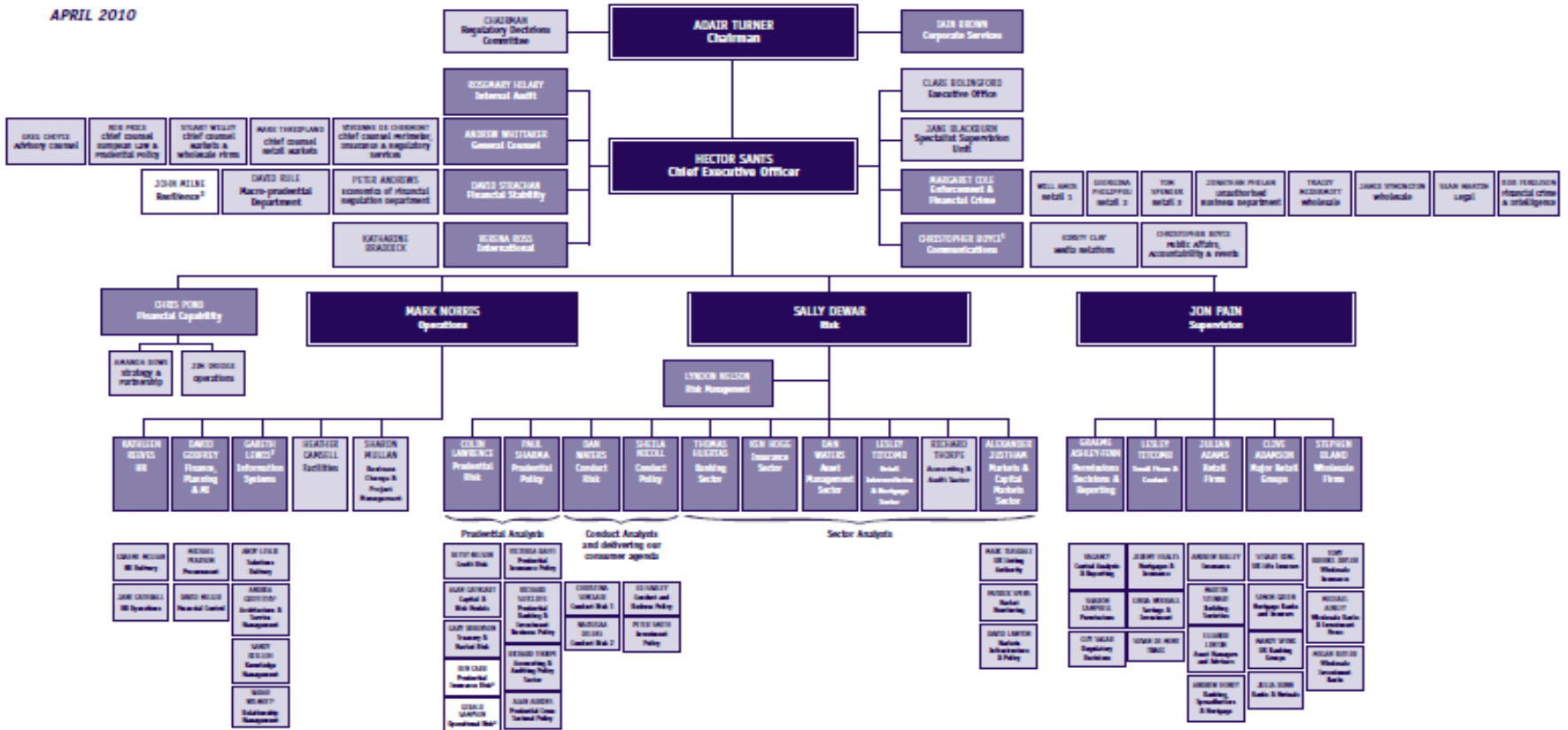
**Prudential Risk Division**

**UK Financial Services Authority (FSA)**

# Topics

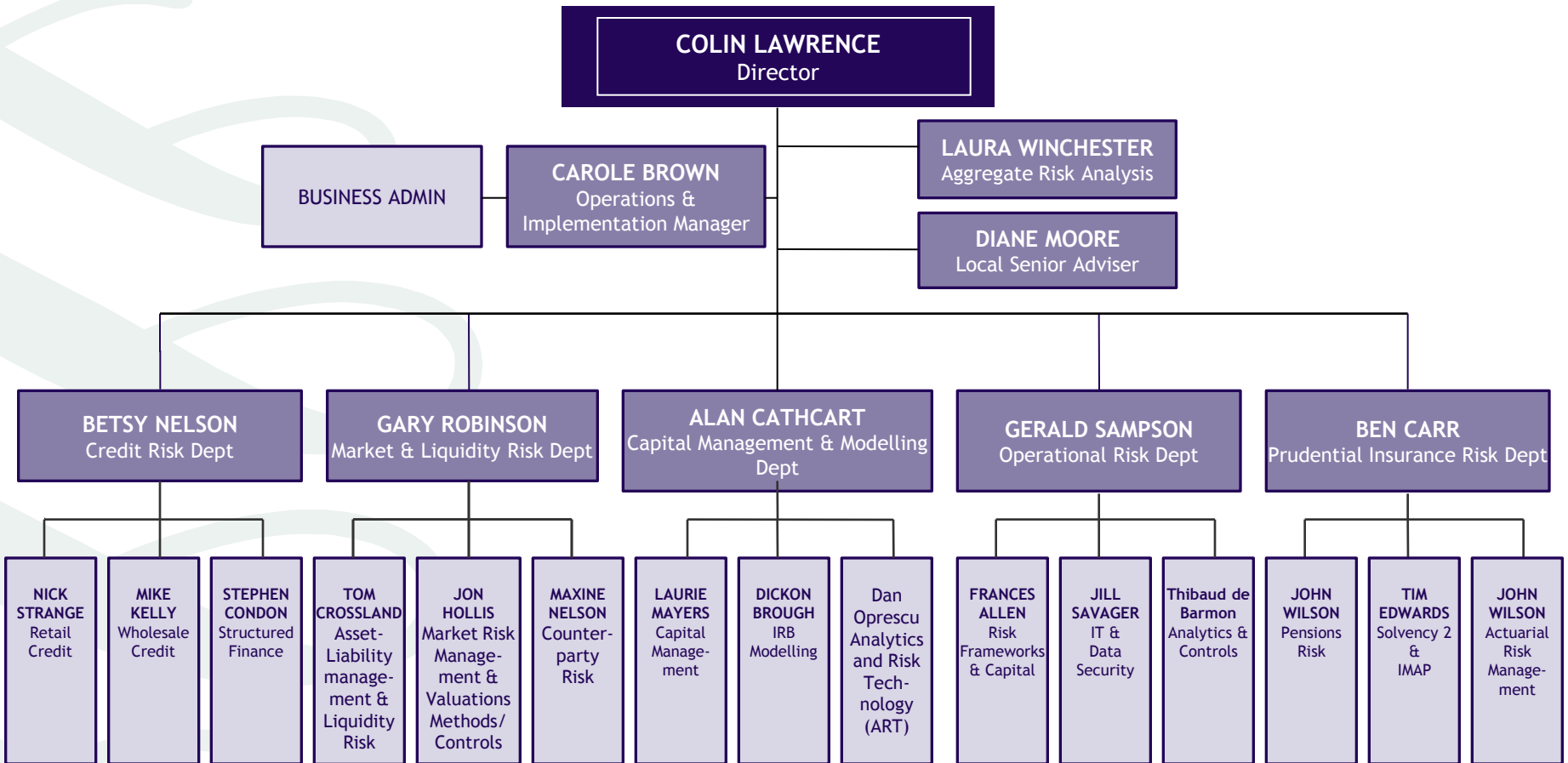
- **Organisation**
- **FSA Handbook and other industry standards**
- **Firm Reviews**
  - ARROW
  - Thematic Work
  - Ad Hoc
  - ‘More Intrusive Supervision’
- **IT Risk Management**
- **Solvency II**
- **Next Steps**

# Organisation - FSA



<sup>1</sup> Acting  
<sup>2</sup> Interim  
<sup>3</sup> Team

# Organisation – Prudential Risk Division



# Organisation – IT and Data Security



- **Currently 6 in the team but recruiting**
  - Headcount will increase to 10
- **All experienced professionals from a variety of backgrounds retail, insurance, markets etc**
  - Understand your position
- **All, except 1, qualified IT auditors (CISA)**
  - Also other qualifications such as ITIL, Prince, CISM, CGEIT
- **‘Shared service’ – work across the FSA on all types of firm**
  - Retail Banks, Investment Banks, Insurers and Market Infrastructure Providers etc.
- **Focus of our work is on high impact firms (circa 70)**

# Organisation – IT and Data Security

## Cont'd



- **Types of work – more later**
  - Support ARROW assessments
    - Including follow up of risk mitigation plans (RMPs)
  - IT assessments for firms seeking Authorisation and Recognition (exchanges and clearing houses)
  - Ad hoc usually incident related
  - Thematic work
    - Data Security in Financial Services 2005
    - Financial Crime Newsletter No 8 2007 – Authentication and Safeguarding of Customer Identity
    - 2009 Survey - Contingency Planning for Retail Deposit Outflows included a section on Internet Banking
    - 2009 Survey - Market Infrastructure Providers Software Resilience

# Organisation – IT and Data Security Cont'd



- **Risk areas covered:**
  - IT Governance
  - IT Strategy
  - IT Risk
  - Business Continuity & Disaster Recovery
  - IT Security – more later
  - Operations & Service Delivery
  - Outsourcing & Offshoring
  - Project & Change Management
  - Data Governance – New(ish) see FSA 2010 Financial Risk Outlook

# Information Security vs IT Security



- **What is the difference?**

- Information Security

- Security of information in all forms (whether held in manual or electronic records)
    - Of interest to both the FSA and the Information Commissioners Office (ICO)
      - ICO penalty power recently increased
      - FSA & ICO liaise on individual issues and cases to decide who is best placed to investigate and use their enforcement powers if necessary

- IT Security

- Subset of Information Security relating to records held in electronic form the outcome of which is to secure the confidentiality, integrity and availability of data and information.

# Organisation – International Angle



- **Lots of interaction**
  - Policy e.g. Solvency II
  - Firm specific – college or bilaterally
  - Topic specific
    - Basel Standards Implementation Group on Operational Risk (SIGOR)
    - Senior Supervisors Group – Risk Management
    - IT Supervisors Group
      - International – meet annually
      - European – meet annually
  - Regulator to regulator – various levels
- **Some harmonisation such via EU Directives; but differences between legal regimes mean complete harmonisation highly unlikely**

# FSA Handbook

- **Key handbook sections (for IT)**
  - Systems and Controls (SYSC)
  - Prudential Standards (GENPRU, BIPRU, INSPRU, MIPRU etc)
- **Rules (must do) and Guidance (should do)**
- **Limited IT related Rules or Guidance**
  - Business Continuity (SYSC 3.2.18 & 4.1.6-8)
  - Outsourcing (SYSC 8.1 & 13.9)
  - Processes and Systems (SYSC 13.7.1)
  - Risk Management systems (BIPRU)
- **No immediate plans to change but...**

# Other Industry Standards

- **Plenty out there:**
  - COBIT
    - VAL IT
    - RISK IT
  - ITIL
  - British Standards e.g. BS25999 – BCP
  - International Standards e.g.
    - ISO38500 – IT Corporate Governance
    - ISO27001 – Information Security Management
  - Prince 2 and Managing Successful Projects
  - PCI-DSS

# Other Industry Standards cont'd

- **FSA Publications**

- Data Security in Financial Services 2005 (technical) – many findings still relevant
- Business Continuity Management Practice Guide 2006 – output from 2005 Resilience Benchmarking exercise
- Financial Crime Newsletter No 8 2007 – Authentication and Safeguarding of Customer Identity
- Feedback Statement on Resilience Benchmarking 2008
- Data Security in Financial Services 2008 (non technical) by Financial Crime Division
- Resilience Benchmarking – Insurance Sector 2010

- **FSA gets comfort where we see the Industry standards and FSA publications being used**

# Firm Reviews

- **Three basic types of review**
  - ARROW (Advanced Risk Responsive Operating frameWork)
    - Full
    - ‘Lite’
    - ‘Very High Impact Firms’ (not yet in place)
  - Thematic (part of ARROW)
  - Ad Hoc – usually incident related e.g. HBOS Data Centre Power Failure in November 2009 and Barclays ATM Fraud in September 2009 or related to large IT Projects

# Firm Review - ARROW

- **Assessed according to the risks they present to our statutory objectives in terms of impact and probability**
  - market confidence - maintaining confidence in the financial system;
  - public awareness - promoting public understanding of the financial system;
  - financial stability - contributing to the protection and enhancement of the UK financial system (new – Financial Services Act 2010)
  - consumer protection - securing the appropriate degree of protection for consumers; and
  - the reduction of financial crime - reducing the extent to which it is possible for a business to be used for a purpose connected with financial crime.
- **Low impact firms are managed via a contact centre and have to make regular returns to the FSA which are monitored**

# Firm Review - Arrow cont'd

- **Medium and High Impact firms are relationship managed**
- **Regular risk assessment of a pre-defined set of 54 risk elements e.g. IT systems**
- **The risk assessment involves interaction with the firms**
  - Information requests
  - Information review
  - Visits / meetings with key firm personnel
    - For a high impact firm there can be in excess of 100 meetings as part of a ARROW risk assessment
- **Independent internal FSA process to validate the risk assessment**
- **High Impact firms (circa 70) are also monitored on an ongoing basis via a process called 'close and continuous'**
- **'Lite' is a scaled down version of a full ARROW**
- **Thematic work is horizontal work assessing cross cutting risks involving several firms or a whole market**
  - **Can undertake thematic mitigation, e.g.:**
    - Dear CEO letters
    - Rules changes
    - Newsletters

# Firm Review - Arrow cont'd

- **‘More intrusive supervision’**
  - Phrase used by FSA in the aftermath of the financial crisis
    - Enhancement of the skills of the FSA and in particular the Supervisory teams
    - Increased use of specialist teams such as those in Prudential Risk
    - Focus on ‘outcomes’ and not just compliance with rules
    - Challenge firms judgements
  - Credible deterrent – Enforcement
    - Use full range of powers – increasing censure and fines for firms and senior firm management
      - Recent fines and ban of senior management at Northern Rock for providing inaccurate information to the firms Board and the FSA

# Firm Review - Arrow cont'd

- **‘Very High Impact Firms’**
  - It will apply to a very limited number of very high impact firms
  - More continuous version of ARROW being planned to cycle through key risk elements throughout the supervisory period (complementing the Arrow risk assessment visit)
  - It will involve reviewing in greater depth the effectiveness of governance and risk management, the sustainability of business models, and liquidity and capital stress-testing (including "deep dives" into portfolios etc)
    - Longer on-site visits to firms
  - More will be formally published in due course

# Firm Review - Arrow cont'd

- **Common areas of weakness:**
  - Legacy systems and IT complexity (larger firms)
    - Ability and cost of support
    - Lack of flexibility and in particular ability to aggregate data
  - Profile of IT in the firm
  - Lack of formal IT governance forums
  - Governance forum skills
  - Checking policy compliance
  - Pressure on IT spend (support vs growth)
  - Effective measurement and reporting of IT related events

# Firm Review - Arrow cont'd

- **Common areas of weakness cont'd:**

- Access controls particularly joiners, leavers and movers
- Unencrypted data
- Relationship management of 3<sup>rd</sup> parties
- Exit plans (outsourcing)
- Penetration testing
- Segregation of duties
- Use of CAATS by Internal Audit functions
- Embryonic Operational Risk Management

# IT Risk Management

- **IT Risk Management is a subset of Operational Risk Management**
  - Basel definition – “The risk of loss resulting from inadequate or failed internal processes, people and systems or from external events.”
  - Whether Basel (EU – Capital Requirements Directive) applies or not the management of IT Risk is expected

# IT Risk Management cont'd

- **How?**

- Not formally defined by Rules and Guidance even for CRD firms
- Assessments need to have a forward looking element
  - Just because it hasn't happened doesn't mean it won't
- Risk and Control Self assessments are common
  - Measure impact and probability
  - Product, process or scenario
- Internal losses can be used
  - Backward looking
- Challenges
  - Measurement
  - Limited by memory and biases

# IT Risk Management cont'd

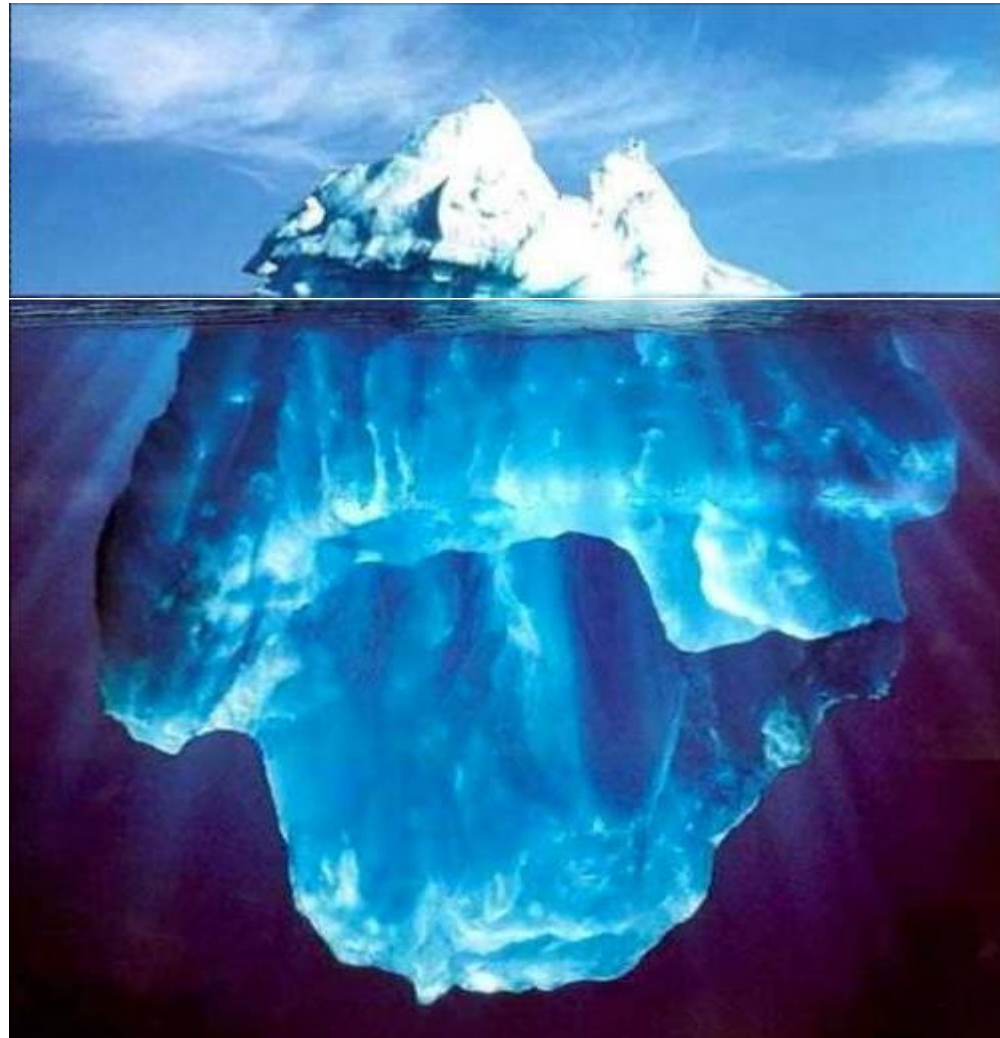
- **Good practices**

- Formal IT risk assessment process
- Link to risk appetite
- Independent challenge
- Regular:
  - Review / update
  - Monitoring
    - KRIs, KCIs, KPIs
    - Trend analysis
  - Reporting to appropriate governance committees
- Use of internal and external information and data
- Operationalised
- Feeds in to Operational Risk and enterprise-wide risk assessment

# Solvency II

Lots of focus on  
internal models

Self assessment,  
reporting,  
governance, risk  
management  
systems, .....



# Solvency II cont'd

- **Reporting**

- No more FSA returns

- New forms

- First report required

- Quarterly report @ 31.12.12 - Within six weeks

- Second report required

- Annual report @ 31.12.12 - Within 20 weeks

- Deadlines reduce over time:

- Quarterly report within four weeks

- Annual report within 14 weeks

# Solvency II cont'd

- **Governance**
  - Data model
  - Platforms
  - Multi-functional teams
  - Documentation
  - Controls
    - Spreadsheet based systems
    - Security

# Solvency II cont'd

- **Data needs to be complete, accurate and appropriate**
  - Low tolerance for errors; recent Northern Rock fine & censure
- **Risk management likely to require links to multiple systems**
  - Data warehouse vs other e.g. spreadsheets
    - Security concerns
- **Level of and control over ad hoc adjustments**

# Solvency II cont'd

- **Learning from Banks – from Capital Requirements Directive**
  - “Meeting FSA data requirements, especially those relating to data consistency and granularity necessitating the **building of a very significant IT infrastructure**”
  - “The acceleration of programmes within a short period, necessitating the **use of a large number of external contractors (especially IT contractors) at inflated rates**”
  - “**The main components of the implementation costs were identified to be IT systems and data collection costs**, as well as the costs associated with the design or enhancement of rating systems and related training and change management. IT systems were found, by the Datamonitor study, to account for over half of the total costs....”

# Next Steps

- **Recruitment**
- **Continued development of Solvency II in preparation for implementation**
- **Development of the ‘very high impact firms’ ARROW assessments**
- **Increasing discussions within the regulatory community**
- **Increasing cross firm meetings**
  - The Managing Director of Risk BU (Sally Dewar) has started a regular CRO forum
  - This is being extended and a forum for Heads of Operational Risk is being considered
  - Where next ?

# Any Questions?

**Jill Savager**

**[jill.savager@fsa.gov.uk](mailto:jill.savager@fsa.gov.uk)**

**020 7066 2304**