

# Governance and Risk Management

Clive Longbottom,  
Service Director, Quocirca Ltd

- Legal Governance:
  - Commercial
    - PAYE, NI...
  - Horizontal
    - Companies Act, DPA, ...
  - Vertical
    - MiFID, FDA, CAA, WEEE, RoHS, CoSHH,...
  - Foreign
    - SOx404, country specific DPAs
- Much legal governance is driven politically – and can change
- But it's not just legal....



- Internal Governance
  - HR
  - Inventory
  - Sales & Marketing
  - Six Sigma
  - ITIL/CoBIT
  - ISO 9000/14000
  - ISO 27001
- Flexibility is key to ensure that internal processes can change to meet market needs
- But there's more....

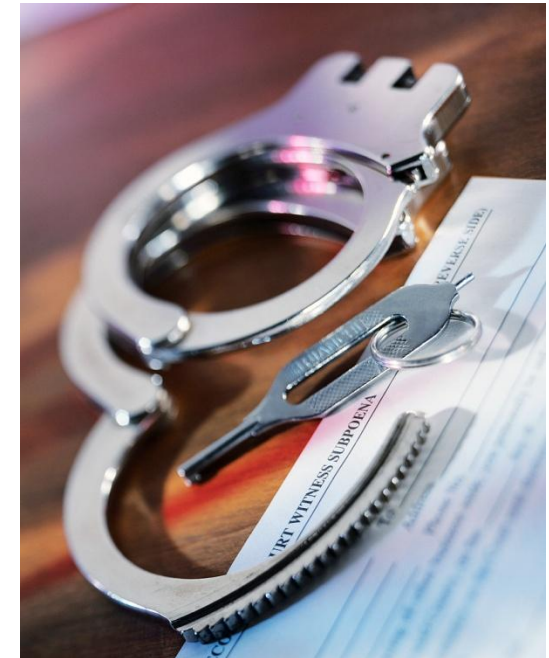


- Value Chain Governance
  - Intercompany transactions
  - Funds clearance
  - Contract negotiations
  - ISO9000/14000
  - ...



- Value Chain Governance must be flexible and inclusive – open standards are key
- It's a minefield – and yet we have to do it

- Legal compliance is subject to checks
  - Who is allowed to see what?
  - Should your own administrator(s) see everything?
  - What can an inspecting body demand to see?
  - What can they take away with them?
  - What do disclosure laws mean?
- Many silo-based compliance solutions mean that you are out of compliance in other areas



- US went overboard
  - SOx, HIPAA....
  - Jeff Skilling, Sanjay Kumar
  - “Safe Harbor” statements
- Europe far more pragmatic
  - Local v. regional v. “Global” laws
  - Risk assessment approach
- Is it possible to be pragmatic yet all inclusive at the same time?



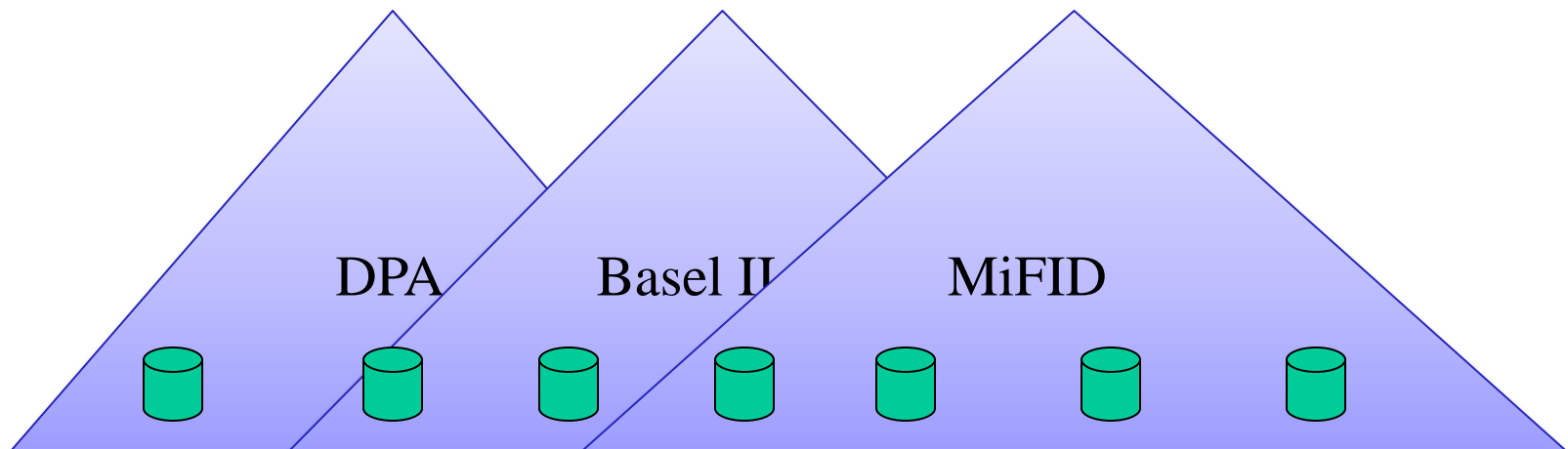
- Governance is often perceived as a bottom line cost
- Business Value Approach
  - Better control of information intellectual assets
  - Better internal information discovery
  - Better decision making
  - Better capabilities along the value chain



- Risk assessment
  - What risk can the organisation afford to carry?
  - What risk can the organisation not afford to carry?
    - Look to BRAND impact as well as direct financial
      - E.g. Nationwide
- Look to the needs, and find solutions that facilitate those needs
- Don't buy point solutions!



- Replacing silos with silos
  - Specific governance solutions
    - E.g.
      - DPA
      - Basel II
      - MiFID



- Information as Intellectual Property
- The need for:
  - Access to all information assets
  - Granular security
  - Intelligent search and discovery
  - Reporting tools
- A “Built In” rather than a “Bolt On” approach





DPA, Basel II, MiFID



- Formal data stores
  - E.g. DB2, Oracle, SQL Server....
- Formal unstructured data stores
  - E.g. FileNet, Documentum, OpenText ...
- Ad hoc data stores
  - E.g. File servers, local storage
- New data types
  - E.g. Voice, video
  
- All need to be controlled and reported against



- The need to gain control over all the information assets in an organisation
  - Data federation
    - Ensuring that all information can be accessed
  - Storage virtualisation
    - Ensuring that all storage assets can be seen as a single logical entity
  - Domain search
    - Being able to find specific information across all assets – rapidly and effectively

- Each information asset needs to be secured
  - By role
    - Internal and external
  - By context
    - Connection type
    - End point device
    - Location



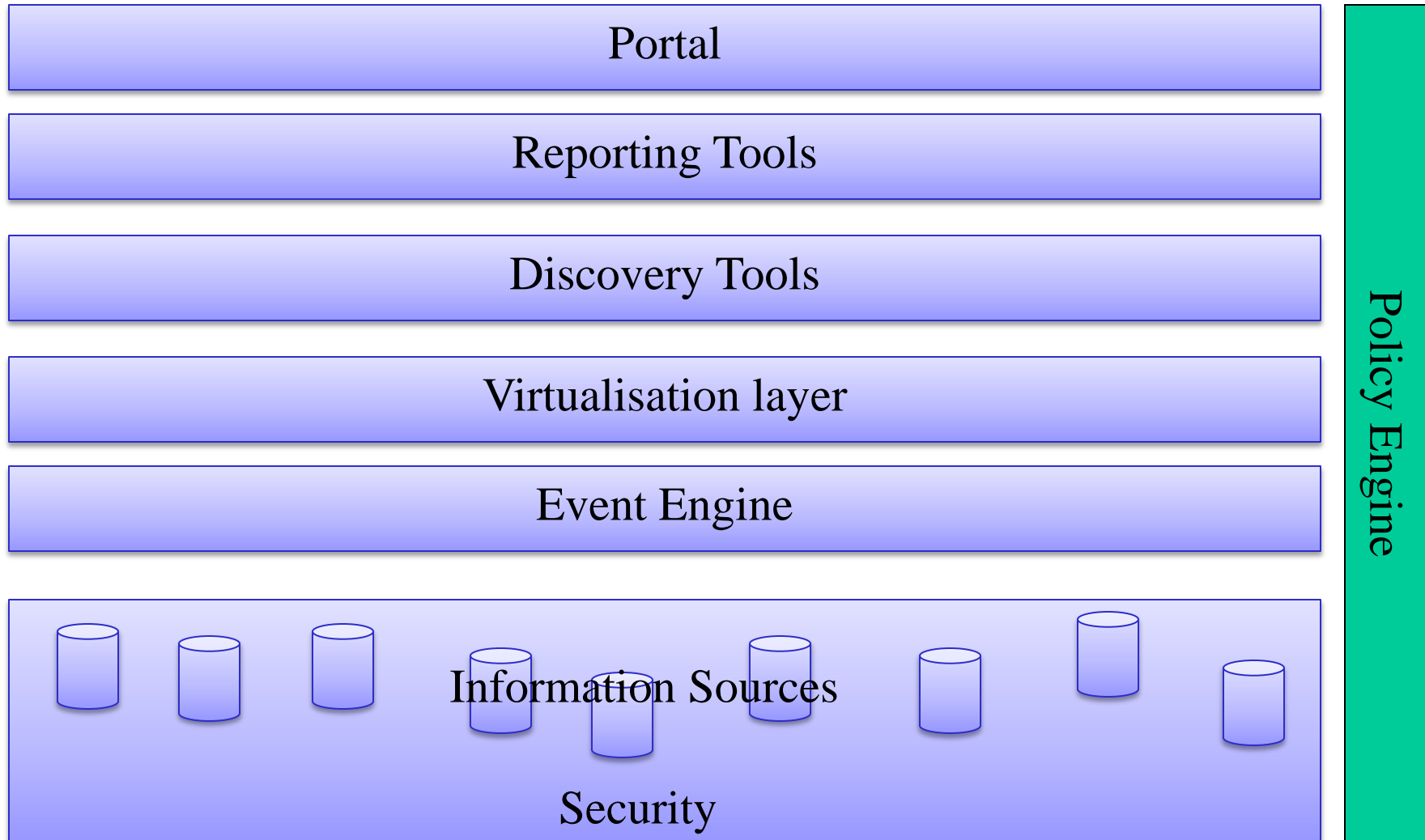
- Each and every action needs to be audited
  - Event engines
    - SNMP
    - XML
    - ...
  - Maintain context of process
  - Ensure that the process can be suitably reported against
    - Who did what, when?
  - Aging of information
    - Ongoing storage
      - Dealing with today's information tomorrow

- The need to report against the underlying assets
  - Aggregation of events and content
  - The need for specific reporting
    - Each governance “flavour” needs different reports
  - Ensuring that people see only what they are allowed to see
    - Internal and external audiences



- The need for reach
  - Governance and Compliance are not “power” plays
  - Each employee, contractor, supplier and customer has their part to play
- Portal technologies provide the capability
  - Open standards provide the reach





- Flexible governance solution
  - Creates an environment that can react to changes in governance needs
- Minimises risk in a risk management approach
  - Governance is “built in”, not “bolted on”
- Opens up capabilities across the value chain
  - Granular security means that information can be more effectively managed outside of the organisation
- Ensures only information that is meant to be seen is seen
  - Policy-based approach maintains content security

- Governance can be chaotic
  - Legal governance can be politically driven
  - Internal and external governance needs to be able to change rapidly
  - One solution can break a previous one
- Bolt on, silo solutions do not solve the problem
  - Each one can break others
- Built in approaches create a Compliance Oriented Architecture
  - Long term, flexible solution for internal and external needs