

## **Data Security**

The Process of classifying securing and monitoring corporate data

**IBM Software** 



**Optimising the World's Infrastructure** 

**27 May 2010** London



#### **Agenda**

- Introduction to Data Security
- Information Flow
- Organising the Effort
- Based on Policy or Standard
- The Data Management Process
- Starts and ends with People
- Importance of Business Process
- Enabling Technology
- Conclusions





**IBM Software** 

# PCTY2010

Pulse Comes to You



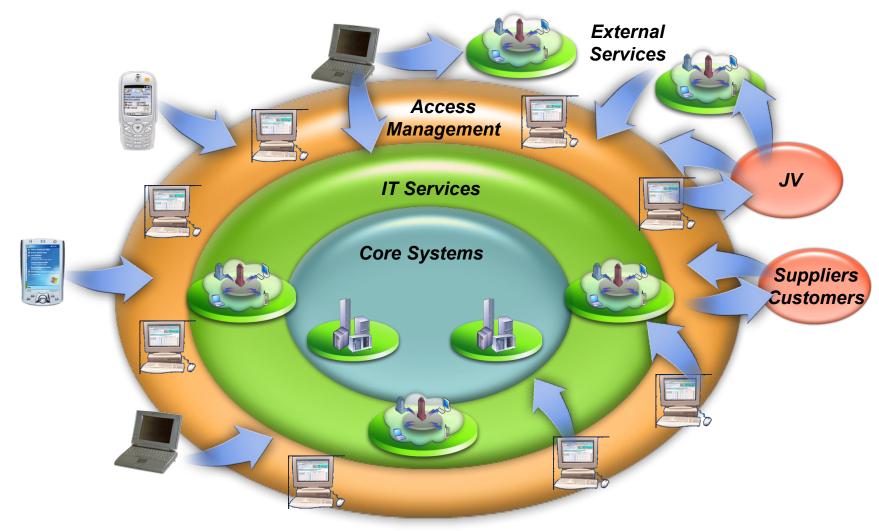
#### **Introduction to Data Security**

- In the modern company information is the greatest asset
- Importance is confirmed with increased regulation
- Embarrassment and reputational damage exposed
- Internal people are often the primary cause of loss
- Consider the Architecture
- Business processes are effected
- Optimised with Technology
- Managed through Risk
- Driven by Policy





#### Information Flow - Collaborative Architecture





#### **Organising the Effort**

- Start and end with Change Management
  - Stakeholder Management
  - Governances structure
  - Changing the hearts and minds of people
- Understand the business and information requirements
  - It is not about prevention, it is about exposing data securely
- Understand the environment
  - Sector based legislation
  - Legislation specific to Data
  - Threat landscape
  - Risk Appetite
  - Existing processes and procedures





#### Related Regulations & Standards

Some of the laws and standards affecting UK organisation:

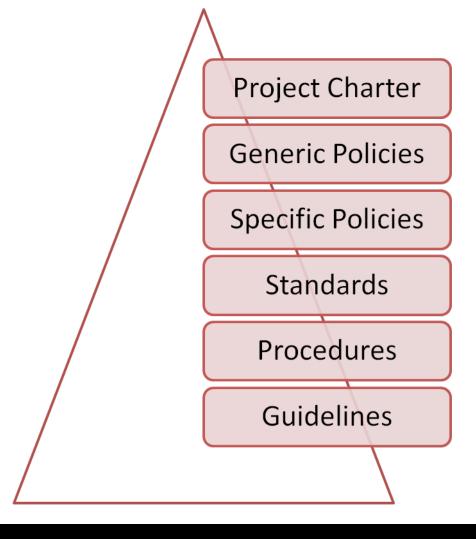
- Data Retention (EC Directive) Regulations 2007 No 2199
- Data Protection Act 1998
- HMG Security Policy Framework
- Freedom of Information Act 2000
- Privacy and Electronic Communications Guide
- Basel II
- Payment Card Industry Standard
- Computer Misuse Act 1990
- ISO/IEC 27001





#### **Based on Policy or Standard**

- Classification of Data
  - Information Classification
  - Business Impact Levels
- Control Framework
  - Annex A from ISO/IEC 27001:2005
  - HMG Information Assurance Standard 1
    - Base line control set (aligned to ISO/IEC 27002:2005)
- Risk Management
  - ISO/IEC 27005:2008





#### **The Data Management Process**

Identification and inventory of Information asset

Identify
Information Asset

Identify Information Owners

Assign responsibilities

Risks associated with information asset

Identify risks of the information asset

Classify Assets based on Risk Appetite Information Asset owner must formally sign off classification level

Apply security controls for information asset

Identify Controls required for Asset

Where improvement is required raise an Observation

Where control is not in place raise a Corrective Action Request

Information
Classification and
Controls Report

Report on mitigation plan

Report on deviations

Report on compliance to policy



#### Starts and ends with People

- History tells us that the vast majority of data losses are because of people within
  - Often this is inadvertent
  - Sometimes without consequence
  - Very seldom is it malicious in nature
- Functional Awareness and Education improves the situation
  - Cultural Reviews
  - Efficiency Reviews
  - Communications
  - Training
  - Written Commitment





#### Importance of Business Process

When people let us down or technology fails business must continue...

- •Business as Usual (BaU) processes must be maintained by the asset owners (or authorised deputy)
- Processes must adhere to policy
- Services based environments must incorporate Service Level Agreements (SLA's) with:
  - Performance based indicators
  - Risk based indicators





#### **Enabling Technology**

You can't manage what you can't measure!

- Security Incident & Event Management (SIEM) can improve your position significantly
- Data Loss Prevention (DLP) technologies will assist in understanding and managing the movement of information
- Governance Risk and Compliance (GRC) tools have some functionality that can assist in stream-lining the process
- Web Services will enable information sharing
- Security technologies are a critical enabler for the implementation of the control framework





#### **Conclusions**

- ✓ Fail or succeed with your people!
- ✓ Business involvement is imperative together with their appreciation of the importance of Data Security
- ✓ Use a proven process or methodology





### **Questions**

