IBM Information Security Lifecycle

Martin Borrett, Lead Security Architect NE Europe, WW Tivoli Tiger Team

Volume of data is exploding

What's driving this tremendous growth?

- Records retention for regulatory and industry compliance
- Data Backup and a Disaster Recovery environment that mirror production data for business resiliency
- Development and test requirements
- Mergers and acquisitions that lead to redundant systems, data centers, applications, etc.

- Technology innovation that makes it possible to access more data, more quickly than ever before

- Data volumes double every 18 months
- 37% of data is expired or inactive
- Information created, captured, or replicated exceeded available storage for the 1st time in 2007
- 70% of the digital universe is created by individuals…
- Average cost of a privacy breach is around $200 per compromised record
- Average US legal discovery request can cost organizations from $150K to $250K

What happens when you're NOT in control of your business data…

"UK NHS - Dozens of women were told wrongly that their smear test had revealed a separate infection after a hospital error, an independent inquiry has found….

…Confusion arose because the hospital decided to use a code number to signify "no infections", not realizing that it was already in use at the health authority where it meant "multiple infections".

"US Supermarket chain - Hackers have stolen 4.2 million credit and debit card details from a US supermarket chain by swiping the data during payment authorization transmissions in stores.

"CHARLOTTE, N.C. – A major US Bank has lost computer data tapes containing personal information on up to 1.2 million federal employees, including some members of the U.S. Senate.

The lost data includes Social Security numbers and account information that could make customers of a federal government charge card program vulnerable to identity theft…."

"FRANCE - Rogue trader accused of the world's biggest banking fraud was on the run last night after fake accounts with losses of £3.7 billion were uncovered. *The trader used his knowledge of the bank's control procedures to hack into its computers and erase all traces of his alleged fraud.*

….Mr Leeson said: "Rogue trading is probably a daily occurrence within the financial markets. What shocked me was the size. I never believed it would get to this degree of loss."

"UK Government dept - Two computer discs holding the personal details of all families in the UK with a child under 16 have gone missing.

The Child Benefit data on them includes name, address, date of birth, National Insurance number and, where relevant, bank details of 25 million people…."

"WASHINGTON – The FINRA announced today that it has censured and fined a Financial Services company $370,000, for making hundreds of late disclosures to FINRA's Central Registration Depository (CRD) of information about its brokers, including customer complaints, regulatory actions and criminal disclosures. *"Investors, regulators and others rely heavily on the accuracy and completeness of the information in the CRD public reporting system - and, in turn, the integrity of that system depends on timely and accurate reporting by firms,"*

What happens when you're NOT in control of your business data…

"UK NHS - Dozens of women were told wrongly that their smear test had revealed a separate infection after a computer error. A public inquiry has found….

Incorrect classification..

Life threatening consequences

…Confusion arose because the hospital decided to use a code number to signify "no infections", not realizing that it was already in use at the health authority where it meant "multiple infections".

"US Supermarket chain has had credit data stolen 4.2 million credit and debit card details from a US supermarket chain by gaining the data during payment authorization transmissions in stores.

Ineffective Security..

Brand damage

Financial loss

"CHARLOTTE, N.C. – A major US Bank has lost computer data tapes containing personal information on up to 1.2 million federal employees, including some members of the U.S. Senate….

Physical Data Loss..

The lost data includes Social Security numbers and account information that may make customers of a federal government charge card program vulnerable to identity theft…."

Identity Theft

"FRANCE - Rogue trader accused of the world's biggest banking fraud was on the run last night after fake accounts with losses of £3.7 billion were uncovered. The trader used his knowledge of the bank's control procedures to hack into its computers and erase all traces of his alleged fraud.

Poor Internal Controls..

Bankruptcy, Financial ruin, penalties

….Mr Leeson said: "Rogue trading is probably a daily occurrence within financial markets. What shocked me was the size. I never believed it would get to this degree of loss."

"UK Government dept - Two computer discs holding the personal details of all families in the UK with a child under 16 have gone missing.

Physical Data Loss..

The Child Benefit data on them includes name, address, date of birth, National Insurance number and, where relevant, bank details of 25 million people…..

Fraud on a massive scale

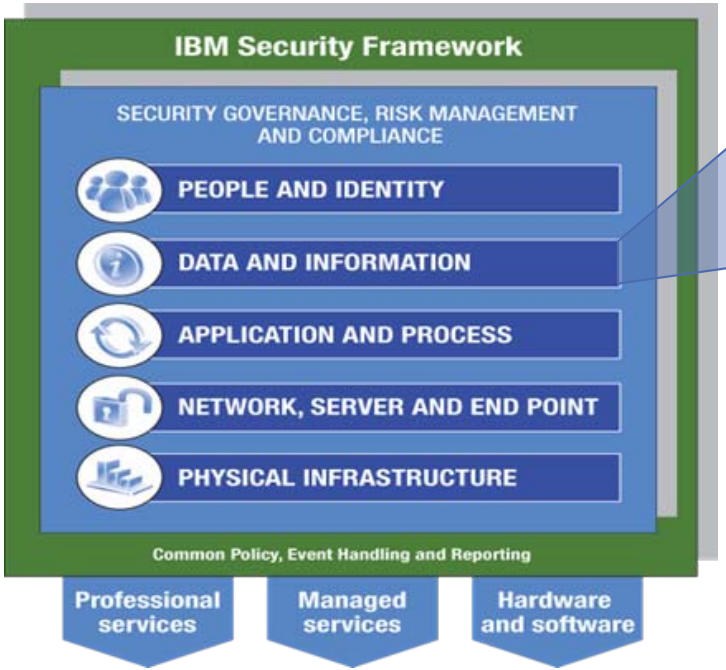
"WASHINGTON – The FINRA announced today that it has censured and fined a Financial Services company $370,000, for making hundreds of late disclosures to FINRA's Central Registration Depository (CRD) regarding its registered brokers, including customer complaints, regulatory actions and criminal disclosures. Investors, regulators and others rely heavily on the accuracy and completeness of the information in the CRD public reporting system - and, in turn, they weigh a firm's decision to rely on timely and accurate reporting by firms."

Late Disclosures..

Heavy Fines

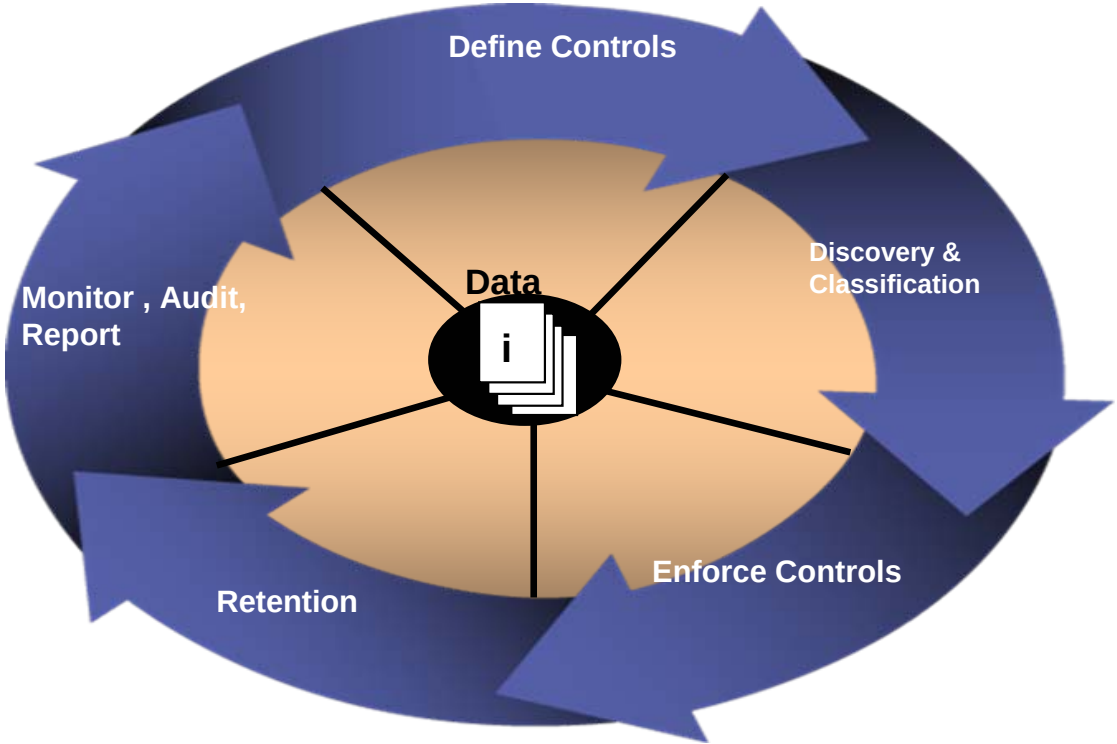
Legal implications and resignations

Information Security Lifecycle



Information Security Lifecycle

is a continuous process of understanding the risks to information and applying a consistent set of controls across the enterprise.



Where do I start when I don't know where the risks are ?

"IT only manages a small percentage of the information floating around our business – we need to have a view that extends beyond traditional IT boundaries – easy to say, hard to do."

Environment

- Official and unofficial data sources being used to make key business decisions
- Many unmanaged data sources
- Web 2.0 projects proliferating with no controls on data sources

Issues

- Unstructured data contained both untapped value and potential exposure issues
- Slow, manual response to legal and compliance audits
- Security teams wanted to put in place controls (messaging, encryption, archiving) but need guidance and prioritization based on risk and value
- No consistent data policies

Data-centric security model

The IBM Data centric security model's purpose is to directly align business strategy and IT security, through the common thread of data. Includes determining enterprise-wide guidelines on data handling based on business policies

Classify Data

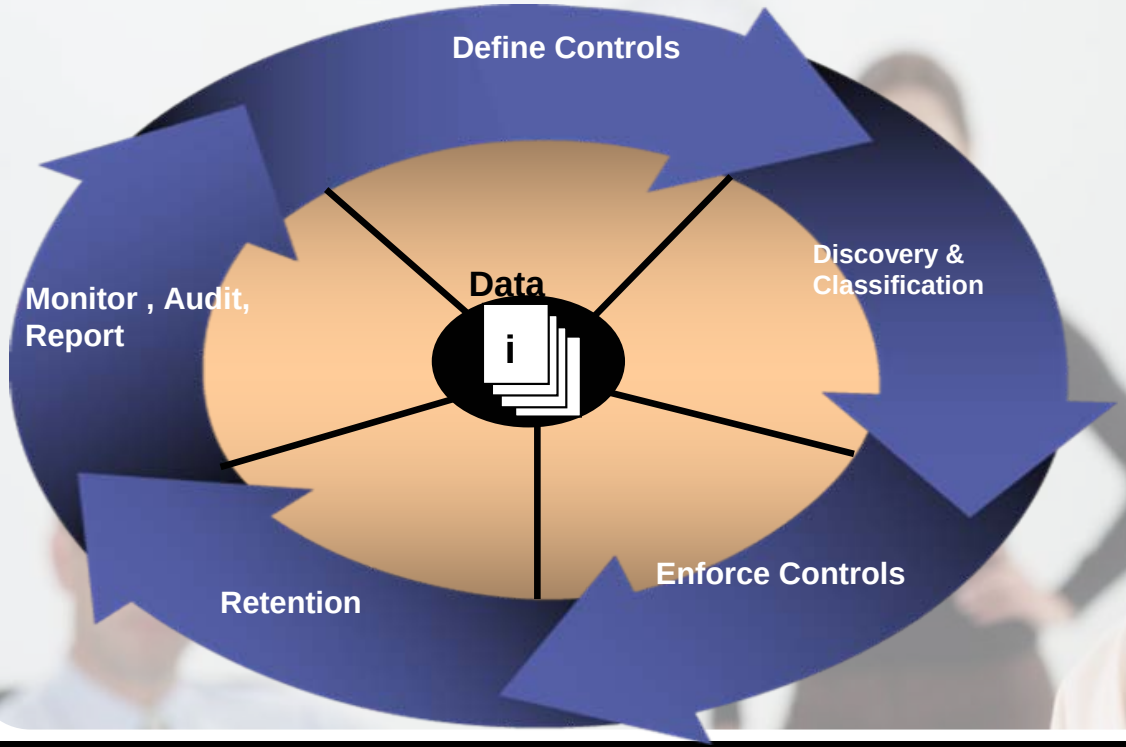
- Where did the data originate?
- Who owns the data?
- Who controls the data?
- Who or what holds the data?
- Who or what can modify or delete the data?
- What type of data is it?
- How sensitive is the data?

Determine policies

- Who or what can use the data?
  - For what purpose?
  - Can it be shared?
  - Under what conditions?
- Where will data be kept?
- How long do we keep the data?
- Does it need to be safeguarded?
  - At rest?
  - During transmission?
  - During use?
- How can data be disclosed?
  - What subset?
  - What protection must be implemented?

Data-centric security model

Acts as foundation to Defining Information Controls



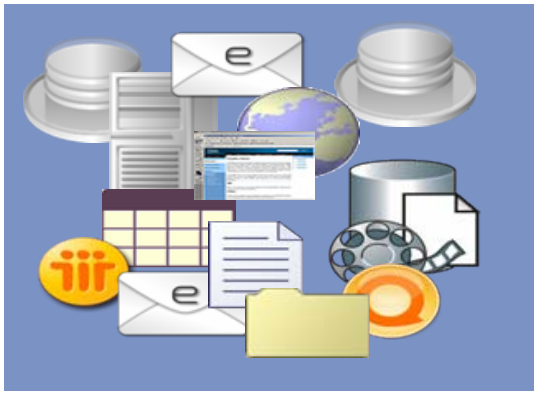
IBM Solutions

- IBM Global Business Services (GBS)
  - Security and Privacy Consulting Services
  - Data Governance Framework, Data Governance Maturity Model
- Cost effective, targeted plan for selecting & implementing security controls based on data value and risk

Discovery & Classification

Decision-making based on the full context

- **Can I automate the process of making consistent decisions about the handling of information without burdening or relying on end- users?**
- **As new information is created, how does the infrastructure know how to handle/treat it?**



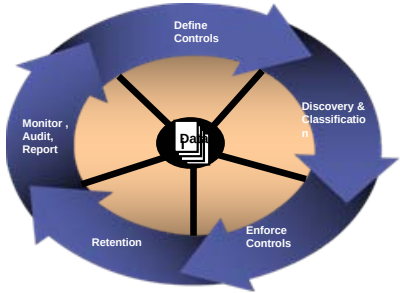
Challenges

- How do I tap the value of value of my data to improve my business?
- Where is my intellectual property stored?
- Affordably supporting eDiscovery requests
- How do I handle the imposing task of records management ?

IBM Solutions

- Data Discovery, and Information Asset Classification Services
- IBM eDiscovery Solutions
- IBM Classification Module

eDiscovery & Classification



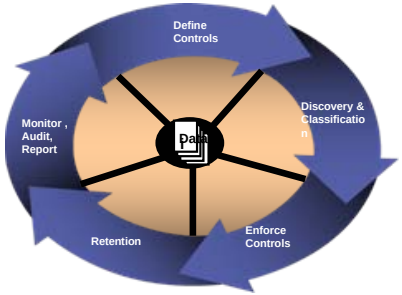
Enforce Controls

Following through on ensuring information is secured according to policy

- Ensure only authorized users can access sensitive information though thoughtful, layered controls
- Guard sensitive information in transit, at rest, or in use
- Manage SLAs for specific information.

IBM Solutions

- ***Identity & Access Management Portfolio***
- Email and messaging security
- ***Database Privacy & Encryption***
- ***Encryption Key Lifecycle Management***
- Tape backup with integrated encryption
- Product Deployment Services
- Data Loss Prevention (DLP) Services
- Most via Managed Data Security Services



How do we protect data from privileged users?

"How can I protect information at the underlying operating system level from unintentional or intentional misuse by root users?

Environment

- Administrators frequently have greater privileges than required, that circumvents other controls
- Root account users aren't uniquely identified, and can alter audit trail
- Privileged users' access not managed according to consistent policy
- **Virtualization** amplifies challenges by dissolving natural separation of duties

"How to Securely Implement Virtualization"
by Neil MacDonald
Gartner Security Summit June 2008

Gartner

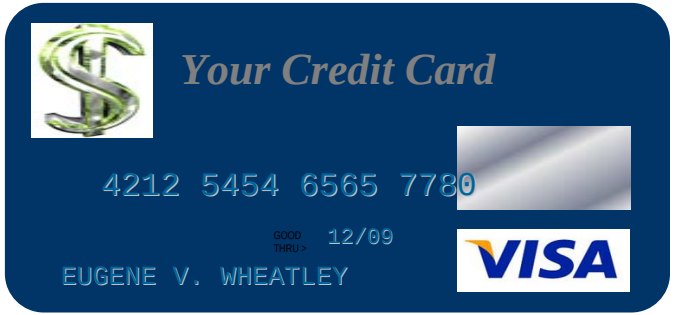
Recommendations for Operating System Access Control:
Tightly control administrative and "root" access
Auditing and logging of administrative activities
Log all activities, link to security information and event management (SIEM)
Ensure security settings can't be altered by operations

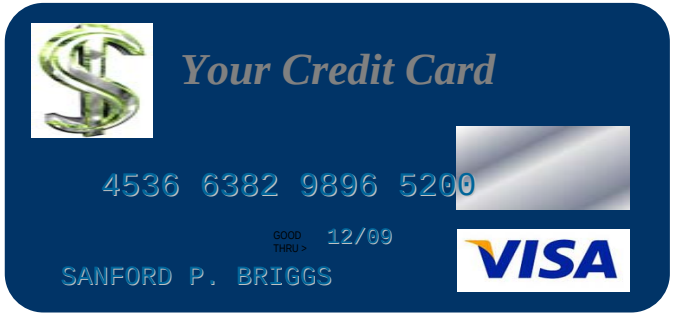
IBM Solution

- ✓**Tivoli Access Manager for Operating Systems (TAMOS)**
- ✓**Granularly sub-dividing root capability for UNIX/Linux**
- ✓**Secured Audit trail, tied to originating identity, integrated with TSIEM Compliance Reporting**
- ✓**Centralized Policy Management, heterogeneous OS environments**
- ✓**Support for virtualization technologies: AIX WPARs & LPARs, Solaris Zones, VMWare for Linux**

Anonymous Production Data

- Removing, masking or transforming elements that could be used to identify an individual
  - Name, telephone, bank account, taxpayer identifier
- No longer confidential; therefore acceptable to use in open test environments
- Masked or transformed data must be appropriate to the context
  - Consistent formatting (alpha to alpha)
  - Within permissible range of values
  - Context and application aware





IBM Solutions

- **IBM Optim Data Privacy**

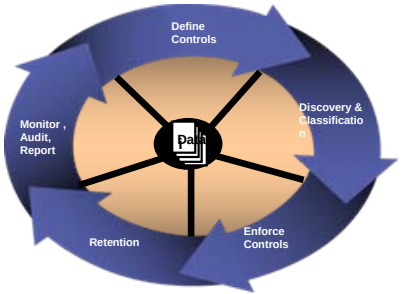
Enforce Controls

Encrypt the Data in your Databases

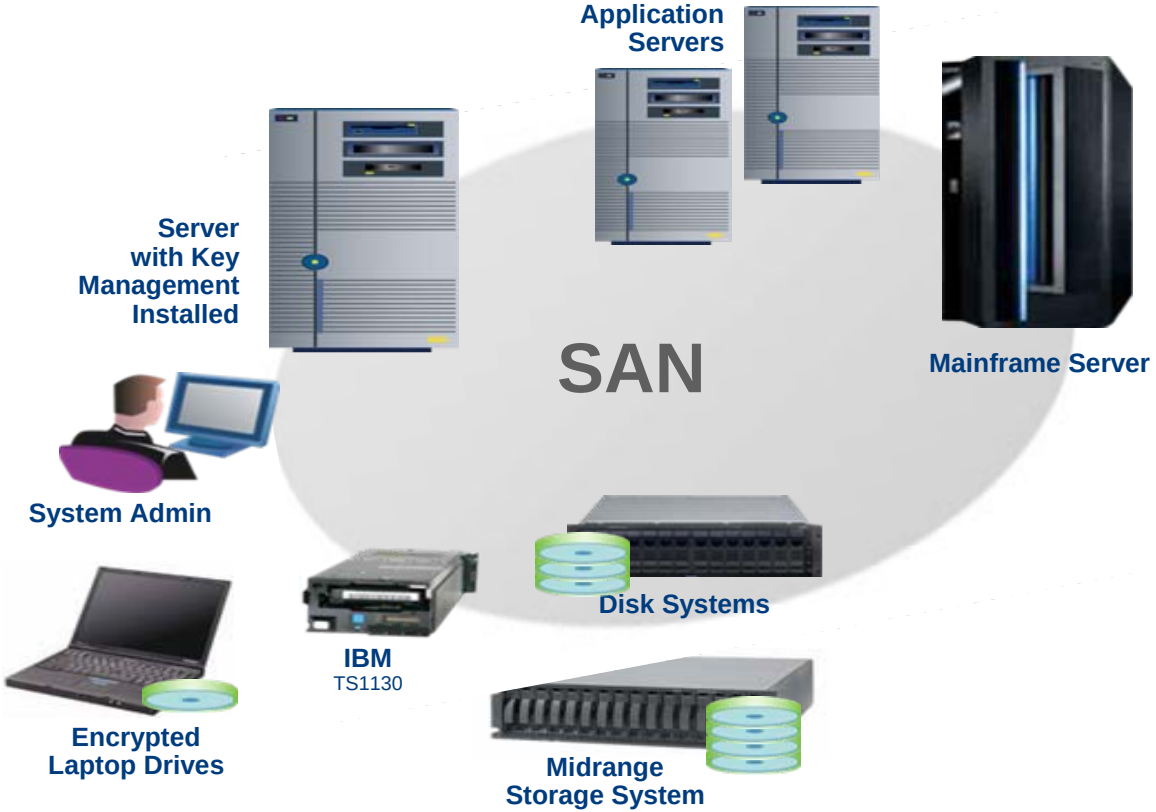
Database Encryption
- High performance database encryption
- Transparency to users, databases, applications, storage
- Available for Distributed DBMS and customized for System/z

IBM Solutions

- Database Encryption Expert for Distributed platforms
- IBM Data Encryption for IMS and DB2 Databases



IBM Tivoli Key Lifecycle Manager & Self Encrypting Tape & Disk



- **TKLM transparently detects encryption-capable media to assign necessary authorization keys**
  - Initially for TS1130, LTO4, DS8000
  - IBM leading standards efforts to expand TKLM to manage Symmetric keys, Asymmetric key parts and Certificates
- **Reduces encryption management costs related to set up, use and expiration of keys**
- **Runs on most existing server platforms to leverage resident server's existing access control, high availability, & disaster recovery configurations**
- **Ensures against loss of information due to key mismanagement**

" What separates IBM from the pack is its ability to provide a complete and extensible data encryption architecture, including an enterprise key management capability."

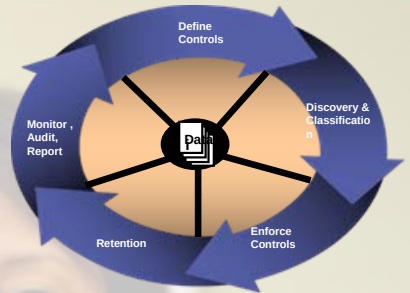
-- Jon Oltsik, Enterprise Strategy Group, Aug. 2008

ESG Enterprise Strategy Group

Data Retention

Managing retention for cost and compliance management

- ***Implement and enforce retention policies to comply with regulations***
- ***Leverage lower cost tiered storage environments for lower valued or inactive data***
- ***Address compliance requirements by protecting information held in non-erasable, non-writable storage***
- ***Improve application or file system performance and shrink backup windows by reducing data size***



IBM Solutions

- Enterprise Content Management
- Optim Database Retention
- Archive and Storage Management
- Continuous Data Protection

Monitor, Audit, Report

Critical data sources mapped to regulatory specific reports

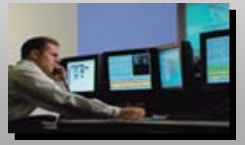
- **Are information controls being enforced?**
- **Understand who is accessing information**
- **Identify any abnormal data access patterns**
- **Monitor security posture of infrastructure supporting information storage and collaboration**
- **Can you provide proof to internal and external auditors?**

IBM Solutions

- **Tivoli Security Information and Event Management (SIEM)**
  - **Controls Monitoring**
  - **Log Management**
  - **Compliance Reporting**
- **Data Security Monitoring and Reporting Services**

Only IBM Offers Complete Solutions to support Information Lifecycle

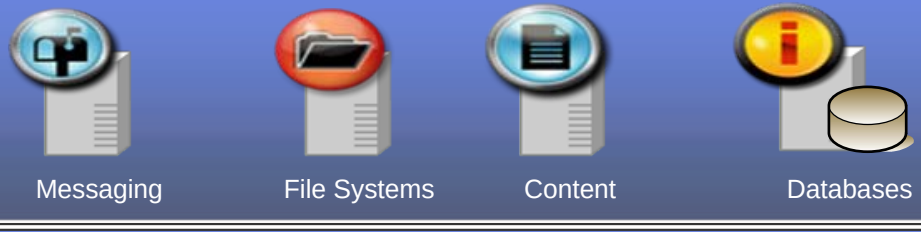
Identity & Access Management



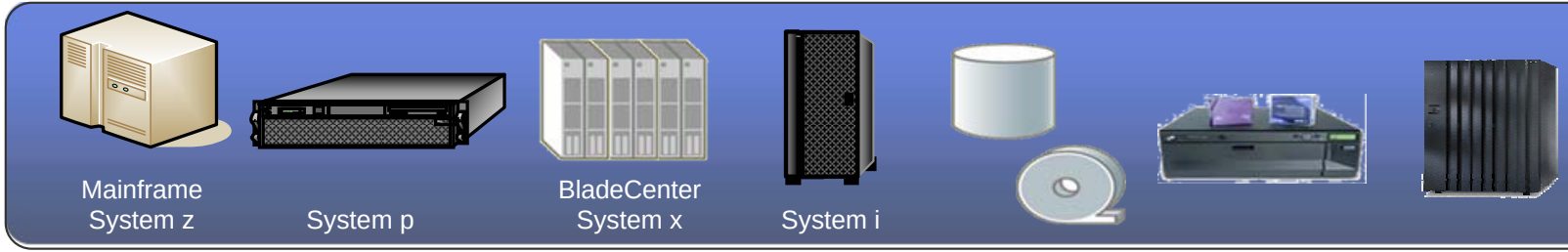
Monitoring & Audit

Consulting, Managed Services, Analytics

Data Management Systems



Platforms



Storage Systems

Data Security Services and Trust Research

Questions?