



One Point Solutions

Information Governance and Security Challenges

Most IT organizations are aware of information governance and security challenges

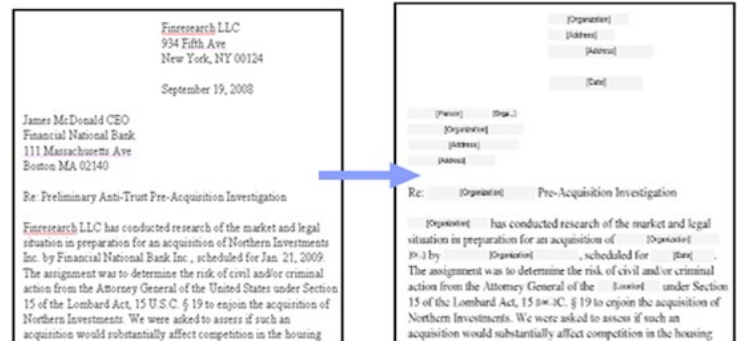
- **Automating compliance** with regulations like HIPAA and SOX.
- **Externally monitoring** sensitive data access and sending real-time alarms.
- Controlling and enforcing **enterprise-wide security models** on-site and in the cloud.
- Protecting sensitive enterprise information -- structured and unstructured -- and **avoid production data breaches** without impacting applications.
- Protecting confidential data used in **test, training and development environments**.
- **Limiting privileged user access** to sensitive data from locations worldwide.
- **Dynamically protecting SQL** from malicious or unauthorized requests.
- **Setting policy-based controls** to detect unauthorized or suspicious activity.
- **Conducting vulnerability assessments**, modifying auditing and blocking rules.
- Additional purchases of hardware storage and CPU to provide for an **increasing volume of production records**.

De-identify Data in Non-Production Environments



Personal identifiable information is masked with realistic but fictional data for testing & development purposes.

Redact data from documents based on established policies to the “cell” level.



Before

After

Inherent Database and System Security is Not Sufficient

- **Privileged users or end-users** override corporate policies, despite defined separation of duties; and can easily modify database log files.
- **No real-time monitoring/reporting** to immediately detect or block unauthorized access.
- **Essential and consistent policy management** tools such as vulnerability assessment, data discovery, leakage detection, file integrity monitoring, and more, are not implemented.
- **Sensitive data** - such as social security numbers, credit card numbers, and salary and health information - is available for global access in test & production environments.
- **End-user fraud** cannot be detected in the application, such as SAP and PeopleSoft, for connection-pooled applications that use generic service accounts.
- **Significant labor cost** to clean & review data, maintain processes.
- Unable to **proactively enforce** separation of duties, implement share policies consistently.
- Data growth management and record retention **processes are manual**.

One Point Solutions

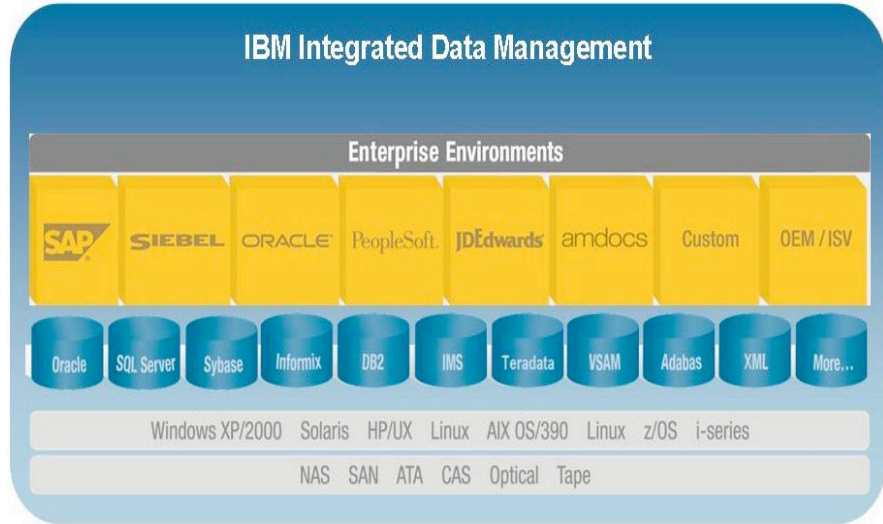


877-3-1POINT x5
admin@one-point.com
OnePointSolutions.com



IBM follows the Information Governance Council Maturity Model

Using the **Information Governance Council Maturity Model**, which was developed with the collaboration of many organizations, IBM Information Governance helps ensure compliance with policy and regulatory requirements, and protect your organization from data breaches.



Information Governance Solutions Using Enterprise-wide controls

- **Locate and document sensitive data** and databases across the enterprise.
- **Identify and classify sensitive data**, such as social security numbers, national id numbers, credit card numbers, salary information, health information.
- **Proactively enforce** separation of duties, implement shared policies consistently.
- **Control data access by cell** (row and column) for both structured and unstructured data.
- **Protect confidential data** in documents while allowing them to be shared.
- **Define / manage privacy and masking rules**, propagate to ensure sensitive data will be protected.
- **Monitor and produce audit and compliance reports** showing actual database access and controls.
- Archive seldom-used records to **reduce CPU and storage costs**, while keeping the records searchable and retrievable.

The Solution: IBM software and One Point's QuickPoint Compliance

One Point Solutions has the expertise to help your organization quickly identify and resolve information governance challenges (not these challenges) using world-class IBM solutions. Our specialists – members of the Information Systems Audit and Control Association (ISACA) – will assist in finding the quickest path to protection using a turnkey appliance-based approach to:

- **Locate, document, and protect data** -- structured and unstructured -- across the enterprise.
- **Define / manage privacy and masking policies.**
- **Install and implement IBM appliances** to provide a peace-of-mind -- and compliance.