

3rd ANNUAL  
**CGOC SUMMIT 2007**

From Planning to Practicing —  
The New Frontier in Retention and Preservation

Sponsored by  
**CGOC** THE COUNCIL  
**PSS** SYSTEMS.

# Retention and Custody

Richard R Gomes, CISSP, CISA, SVP Citigroup Corporate Center/IT Risk

**citigroup** 

The Retention and Preservation Community

## Biography

### **Richard Gomes, CISA, CISSP**

*SVP Citigroup Corporate Center, Operations & Technology/ IT Risk Management Organization; Senior Policy Coordinator, Citigroup, Inc.*

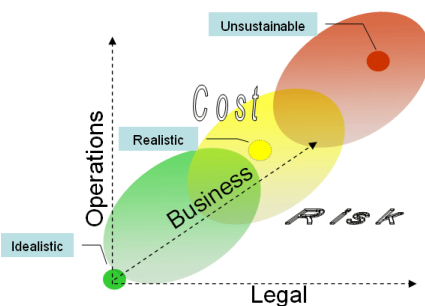
Richard's recent professional focus has been on IS Governance, and he brings a standards and regulatory compliance perspective to the development and pragmatic implementation of IS policies and controls. Richard brings thought leadership, best practices, and established methodology to very large scale strategic initiatives.

## A Quick Reference to the Framework...\*

\*October 18<sup>th</sup> CGOC

Three views combine to describe a record, its location, and its custody

- The Legal view defines Record Class, Code, Retention, and Jurisdiction
- The Business view identifies Ownership, Sensitivity, and Risk
- The Operational view provides Custody, and Logistics



### Cost/Risk Determinants

1. **Legal determines risk:**  
 "What do we need to keep?"
2. **Operations determines cost:**  
 "How do we need to keep it?"
3. **Business determines the equilibrium:**  
 "Where do we focus our efforts?"

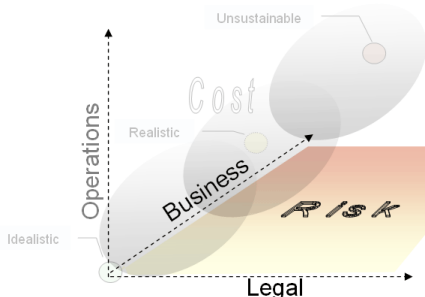
3

## Legal Considerations Drive Retention

\*October 18<sup>th</sup> CGOC

The Role of the Records Catalog: "What do we need to keep?"

1. Specifies Legal and Regulatory Retention Requirements
  - Jurisdictional Considerations
2. Stipulates Accessibility and Conditions
  - Availability, Confidentiality, Integrity



### Business / Governance Activities

1. **Policy & Standards**
  - Risk Based
  - Aspirational not Proscriptive
  - Internally and Externally Aligned
2. **Internal Audit**
  - Risk not Policy
  - Consultative not Punitive
3. **Architecture**
  - Guidance
  - Investment (e.g. shared services)

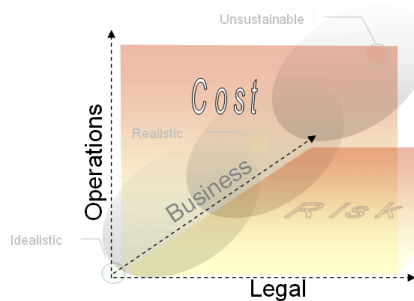
4

## Operational Considerations Drive Cost

\*October 18<sup>th</sup> CGOC

### The Role of the Custody List: "How do we need to keep it?"

1. Adopts the Instance View- *For each record,*
2. Location: *Where is it?*
3. Accessibility: *How is it stored?*
  - Physical Security  $\Rightarrow$  *Availability, Confidentiality*
  - Logical Security  $\Rightarrow$  *Confidentiality, Integrity*



### Business / Capability Costs

1. **Inventory and Tracking**  $\Rightarrow$  **Responsibility**
  - Ownership
  - Stewardship
  - Possession
2. **Preservation**  $\Rightarrow$  **Chain of Custody**
  - Disposal Suspension- Holds
  - Lifecycle Management
3. **Retrieval**  $\Rightarrow$  **Responsiveness**
  - Chain of communications
  - Authorization Keys

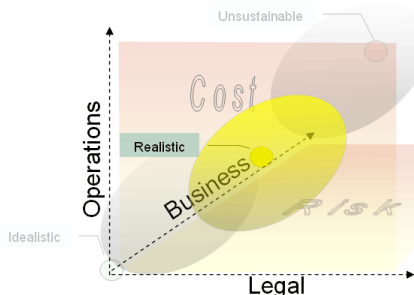
5

## The Business Decides

\*October 18<sup>th</sup> CGOC

### Striking a Cost/Risk Equilibrium

1. Risk Management
  - Formalized risk program owned by Senior Management
2. Cost Management
  - Tied to P&L, and owned by the business heads



### Records Management Program

1. **Risk Drivers**
  - What *must* we do and when?
  - What *should* we do
  - Possession
2. **Cost Drivers**
  - Efficient Business Process
  - Leverage Automation Opportunities
  - Vendor/Service Management

6

## Custody Model – today

We're already managing custody- just not well

1. Spreadsheets Galore (The EUC Solution)
  - **Difficult to administer and manage**
  - **Not well integrated into the process**
    - Passive Solution- *difficult to administer and impossible to maintain accurately*
    - Lack of transparency- *no one knows exactly what we have and who has it*
    - Subject to human error- *few data integrity controls are possible*
- + 2. Processes are Dependent on Record Media and Environment
  - **Physical Records**
    - Rely on 3<sup>rd</sup> party Inventory and Tracking
    - Requires external cooperation to achieve process improvement
  - **Electronic Records**
    - Does not work well with Shared Services Architectures (SSAs)
    - Structured vs. Unstructured information requires very different solutions

### Very Costly

- Labor Intensive
- Prone to overly broad holds
- Not responsive to Legal needs

and

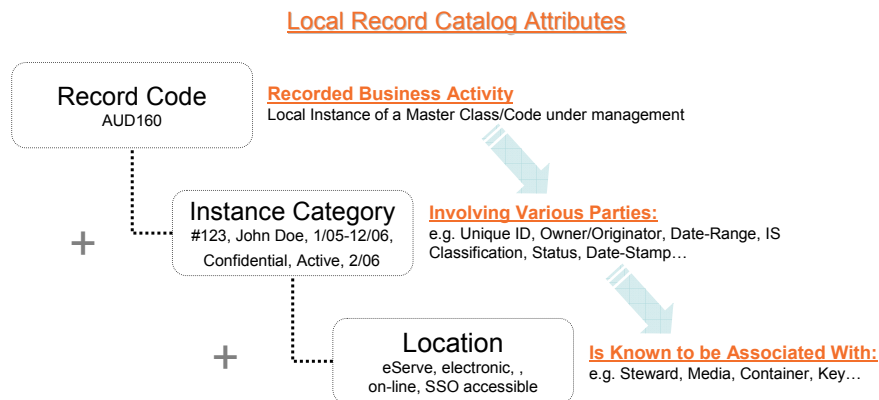
### Risky Solution

- Over retention
- Misplaced records
- Inaccurate custody trail

7

## Custody Model – tomorrow

Custody as an attribute not an afterthought



Significantly Lower Cost and Fully Mitigated Risk

8

## Retention and Custody Model – Summary

**Guiding Principle: Custody Is an Attribute not an Afterthought**

### Significantly Lower Cost and Fully Mitigated Risk

- |   |   |
|---|---|
| <p>1. Discovery and Reporting</p> <ul style="list-style-type: none"><li>• Lower cost of 3<sup>rd</sup> party eDiscovery review</li><li>• No Spreadsheets (EUC overhead)</li><li>• Lower Resource Overhead of Attestation and Audit</li><li>• Direct Attorney ↔ Owner ↔ Steward Communications</li></ul> <p>2. Automation opportunities:</p> <ul style="list-style-type: none"><li>• Retention Management and Enforcement</li><li>• Holds Management and Enforcement</li><li>• IS Control Monitoring</li><li>• Audit and Attestation</li><li>• Vendor and Service Management</li></ul> | <p>1. Discovery and Reporting</p> <ul style="list-style-type: none"><li>• Fewer pages to review</li><li>• Centralized Tracking</li><li>• Auditable Chain of Custody</li><li>• Ownership/Stewardship Linkage Preservation</li><li>• Independent of media or structure</li></ul> <p>2. Automation opportunities:</p> <ul style="list-style-type: none"><li>• eDiscovery</li><li>• Inter-Party Communications</li><li>• Self documenting Holds Management and Enforcement</li><li>• Attestation and Interview Processes</li><li>• Integrity, Availability, and Confidentiality enforcement</li></ul> |
|---|---|

9

## Retention and Custody Model – Questions?

**Guiding Principle: Custody Is an Attribute not an Afterthought**

10