Information Governance and Security Policy - Two Peas in a Pod

Bryn Bowen CRM
Frank LaSorsa CRM
Eugene Stakhov CRM

What is policy ?

Why have an IG Security Policy anyway?

- Compliance
- Competitive advantage
- Expense management
- Solid, secure infrastructure supports growth

Question

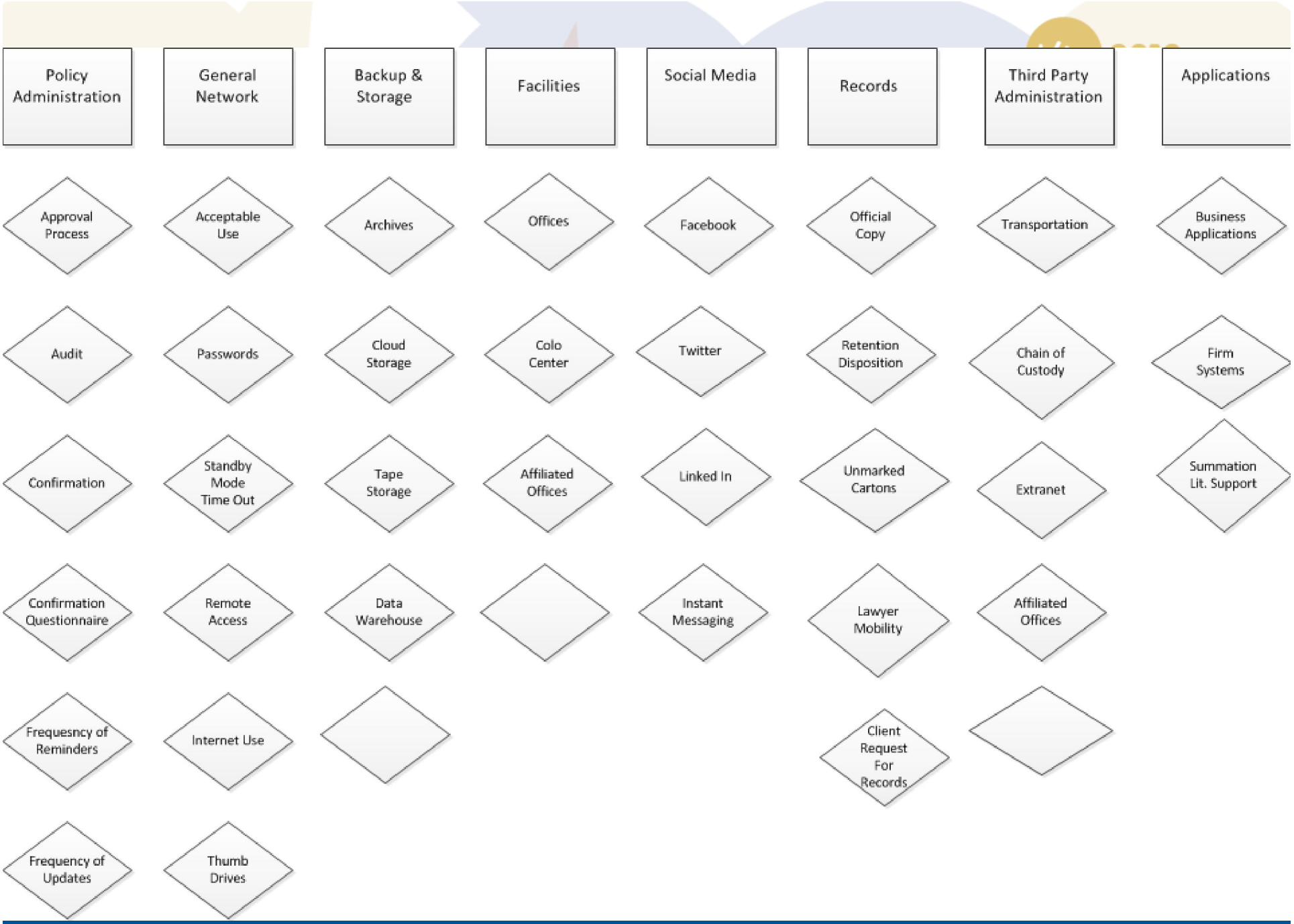
What are the major obstacles you encounter in your organization in trying to create and implement various IG policies ?

What are the major obstacles to creating/implementing an IGS Policy?

- "Culture"
- Management buy in
- Authority to coordinate employees outside of your functional area
- Identifying stakeholders
- Current infrastructure
- Ensuring adoption

Activity

In the envelope you will find various headings (bigger strips). You will also find smaller strips containing terms that would fit under one of the larger category headings. The purpose of this activity is to get you thinking about your policy roadmap.


Policy Administration
General Network
Backup & Storage
Facilities
Social Media
Records
Third Party Administration
Applications
Approval Process
Audit
Confirmation
Confirmation Questionnaire
Frequesncy of Reminders
Frequency of Updates
Acceptable Use
Passwords
Standby Mode Time Out
Remote Access
Internet Use
Thumb Drives
Archives
Cloud Storage
Tape Storage
Data Warehouse
Offices
Colo Center
Affiliated Offices
Facebook
Twitter
Linked In
Instant Messaging
Official Copy
Retention Disposition
Unmarked Cartons
Lawyer Mobility
Client Request For Records
Transportation
Chain of Custody
Extranet
Affiliated Offices
Business Applications
Firm Systems
Summation Lit. Support

How you write is as important as what you write !

Tips and Exercises

What's wrong with this ?

- Some people will react to the increase in the gas tax by taking taxis, buses or other public transportation since these forms of transportation are somewhat less expensive than using a private automobile. However, some people may not be willing or able to make such a change: they might live far from public transportation or might have medical conditions that made it necessary for them to drive. These people will continue driving, but they would generally be likely to take fewer trips than before the tax.

Is this better ?

A higher gas tax would reduce the amount of driving by people who can easily use other forms of transportation. People who can't switch would continue to drive, although they would probably drive fewer miles than before.

Rule #1 – BE CONCISE !

Later, we will be writing some sample paragraphs. These rules will help.

And this ?

It is policy that all employees have computers at their disposal. These are mostly provided for firm business, but use for important occasional personal business is also okay. There will also be software provided that will allow access to the internet, production of documents, access to CD and DVD and databases.

Rule #2 Be Specific

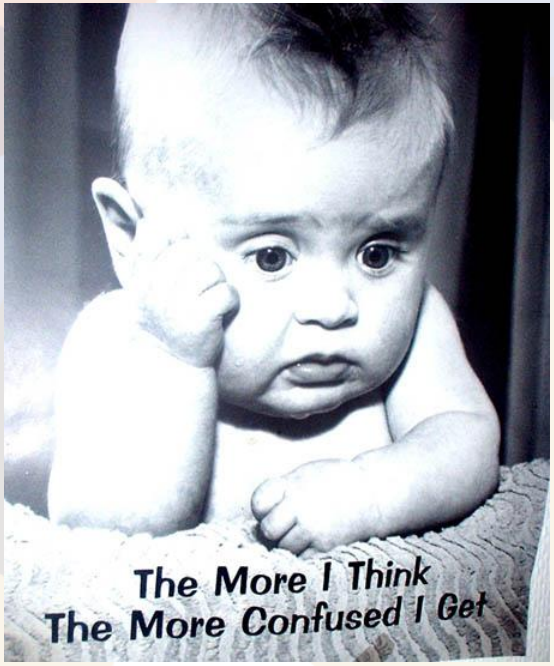
What is occasional personal use ?

Any problems here ?

- The firm requires a dual factor multilayer authentication when accessing via the Citrix gateway. Active director gateway and appropriate certificate clearance is required for said access.

Rule #3 Avoid Jargon

Can you fix the paragraph on the prior slide ? Try it now !



Rule # 4

- Write for the intelligent non-specialist.

Any problem with this policy paragraph ?

After the entire physical and electronic set has been reviewed, the electronic documents will be transferred to a CD or DVD to be sent along with the hard copy to the designated address. If Firm Counsel advises that no copy of the records is to be made, then the right to request these at a later date should be reserved as indicated in the sample release letter below:

Rule #5

Don’t mix policy and procedure.

Procedures lead from policy.

The Policy Guidelines

- #1 Be Concise
- #2 Be Specific
- #3 Avoid Jargon
- #4 Write for the intelligent non-specialist
- #5 Don't mix policy and procedure
- #6 Focus on results (avoid too much detail)
- #7 Identify positive and negative

More Policy Guidelines

- #8 Anticipate questions and problems
- #9 Use tables and summaries
- #10 Include effective date and limitations
- #11 Include acknowledgment and audit
- #12 Provide feedback loop

User Education & Responsibilities

- Consider that protection is now a combined effort of info consumers and managers
- Mitigate risky behavior – how?
- Deter - create enough hurdles, high enough
- Can't lock it down – information feeds the enterprise
- Whose device/information is it anyway?

Taxonomy and Information Governance

A Love Story

Security

- Integral component of IG policy
- Context-sensitive
- Authentication/Authorization
- Distinguish between users, groups and the rights (privileges)

Classification

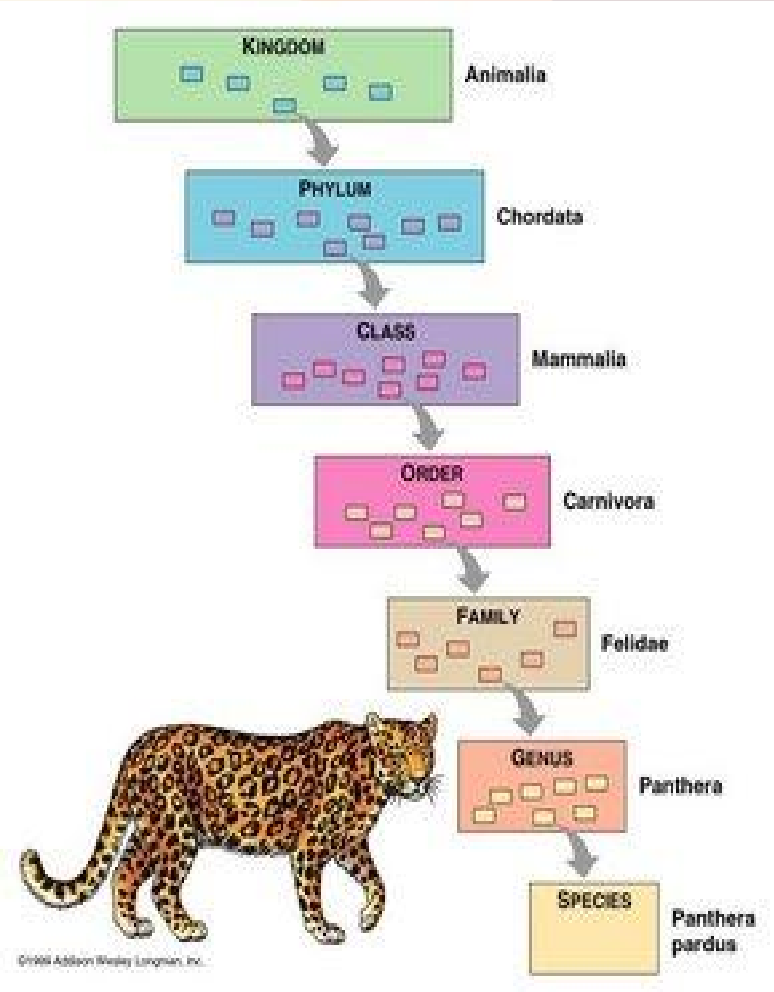
- ECM Mantra: “What you get out is what you put in”
- Assigning metadata to information
  - Tagging
  - Filing
  - Categorizing
- A challenge to implement

Auto-Classification

- Brains vs. Brawn?
- Planning vs. Technology?
  - Artificial Intelligence
  - Information “Crawling”
- AD Group: AccountingUsers
- Records File Plan:

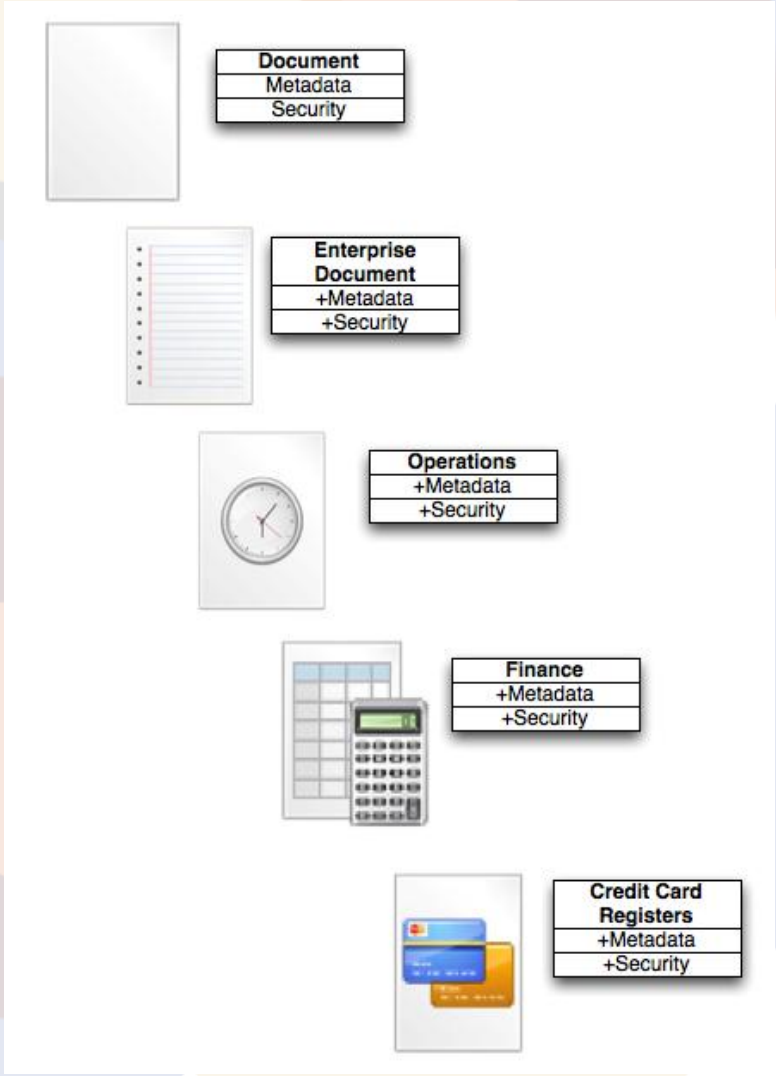
  `//Acme Corp/Finance/Accounting/Receivables/2012-01`
- Harness the Power of Metadata

Taxonomy 101



- Classification
  - Inherit characteristics of parent
  - Add to parent's characteristics
  - Inheritance and Specialization
- Standardization
  - Nomenclature
  - Metadata
  - Structure
  - Relationships
  - Security

Taxonomy 101



- Classification
  - Inherit characteristics of parent
  - Add to parent's characteristics
  - Inheritance and Specialization
- Standardization
  - Nomenclature
  - Metadata
  - Structure
  - Relationships
  - Security

Taxonomy 101

- Objects come from Classes
- Classes contain Properties
- Classes contain Sub-Classes

Taxonomy 101

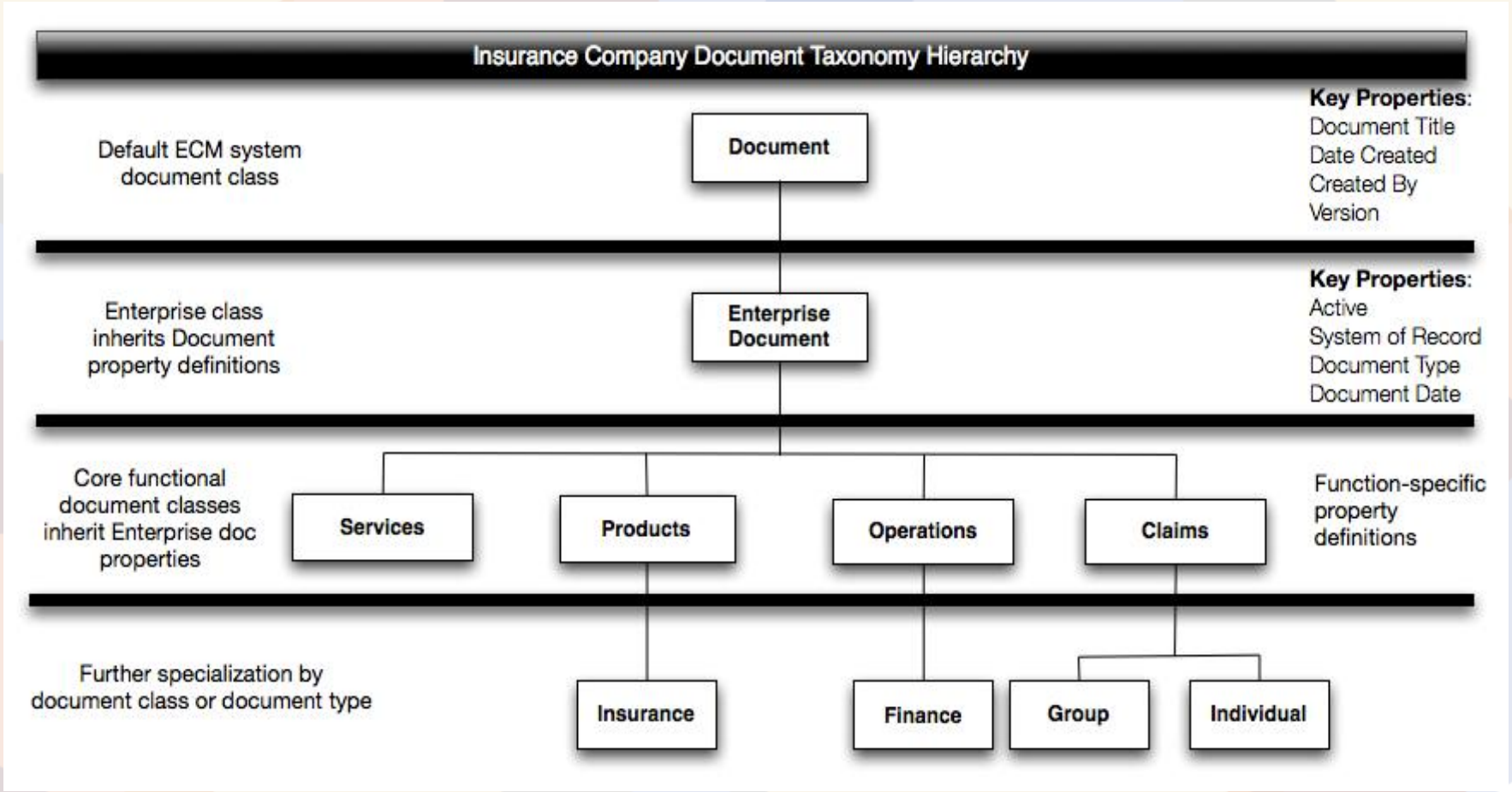
- Objects come from Classes
- Classes contain Properties
- Classes contain Sub-Classes

Geek Alert:

Object-Oriented Programming

- Inheritance
- Polymorphism

Taxonomy 101



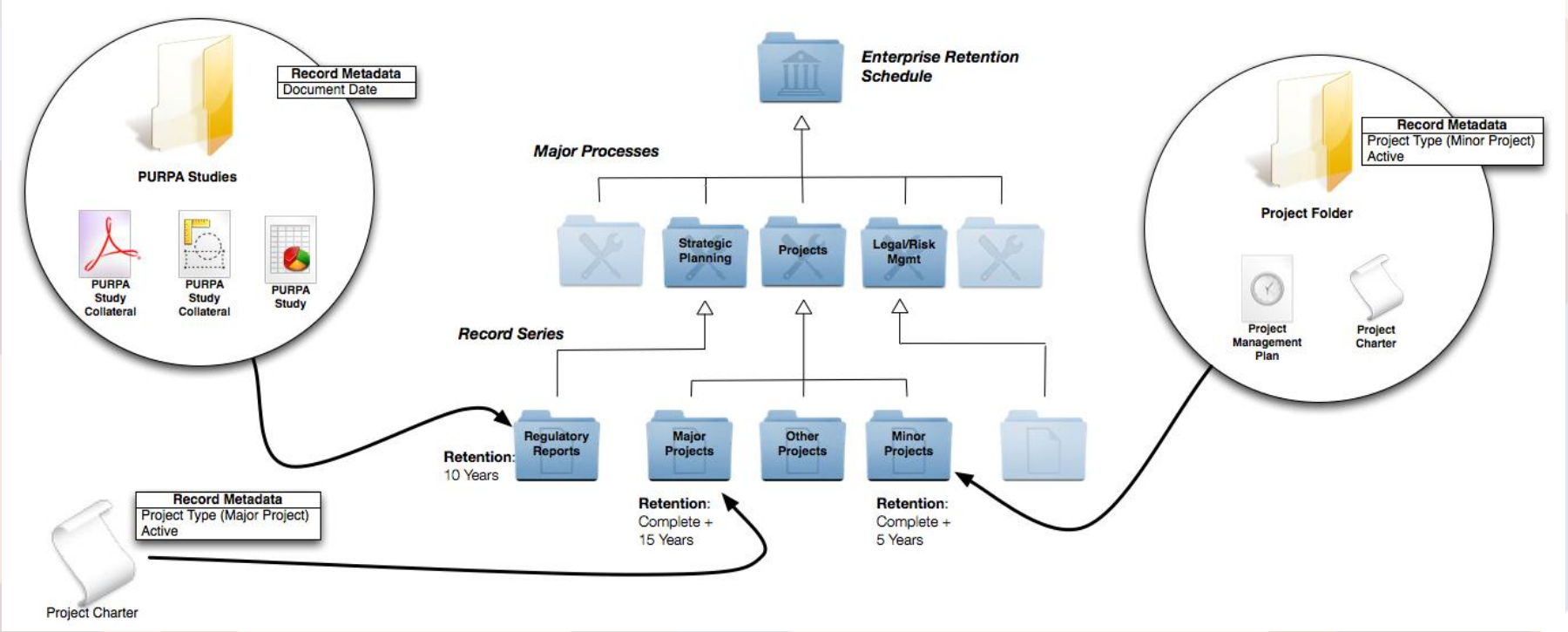
Taxonomy 101

High-Level Target Specifics

- Design Style Choices (Enterprise)
  - Content Centric
  - Organizational
  - Functional
- Design Granularity
  - Item Type vs. Document Type
  - Access Requirements
  - Records Management
- Properties
  - Centralization
  - Polymorphism

Records Management

Sample File Plan Mapping



Building Tools

- Taxonomy Definition Matrix
  - Search
  - Lifecycle
  - Reporting
  - Process/BPM
- Enterprise Property Listing
  - Property dictionary
  - Full metadata
  - Choice lists
- Process Worksheets
  - Qualitative

Lowering the Barriers to Effective Classification

Universal Ingestion Tool - Demo

Standards and Policies - Intersection

Main Standards to Consider:

MoReq2

ISO 15849

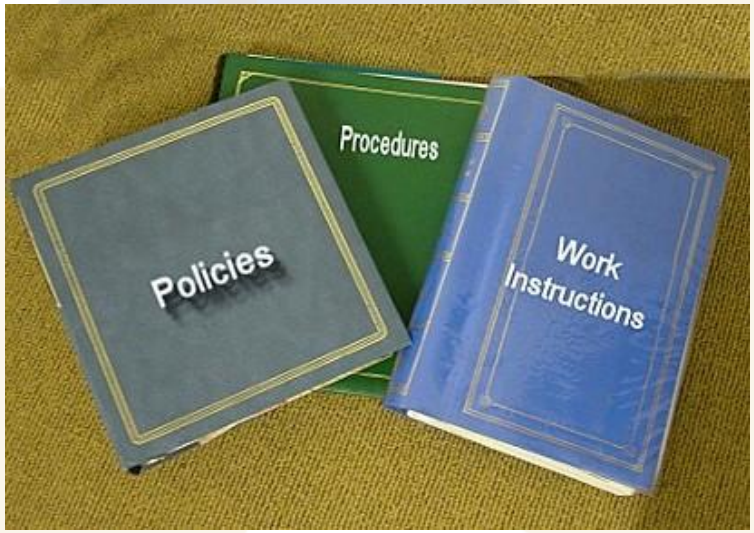
HIPAA

HITECH

ISO 270001

Standards & Policies - Intersection

- Does your policy address/incorporate these standards?
- What is the gap, and how do I identify it?



Standards and Policies - Intersection

- 27001 Highlights:
- Security v. Mobility – is there a winner ?