Protect Your High Risk Information – An Approach to Enterprise Information Mapping

ARMA Triangle Chapter

Raleigh, North Carolina

December 3, 2009

Maura L. Dunn, CRM, PMP
Duff & Phelps, LLC

DUFF & PHELPS

Agenda

- Key Drivers
- Approach
- Case Study

In today's information-driven, fast-moving and highly competitive business environment, organizations face a number of information challenges

High Profile Drivers

Litigation

- **Growing likelihood of high-value litigation**
- **Increasing volumes of electronically stored information leading to increasing costs of preparing for and responding to litigation**

Privacy

- **Increasing pressure to better manage Personally Identifiable Information (PII) based on potential fines, disciplinary action and negative impact on reputation for mishandling (accidental or intentional)**

Mergers, Acquisitions and Divestitures

- **Greater need to provide transparency throughout the process**
- **Growing importance of good information management practices to ensure post-transaction integration success**

Intellectual Property Protection

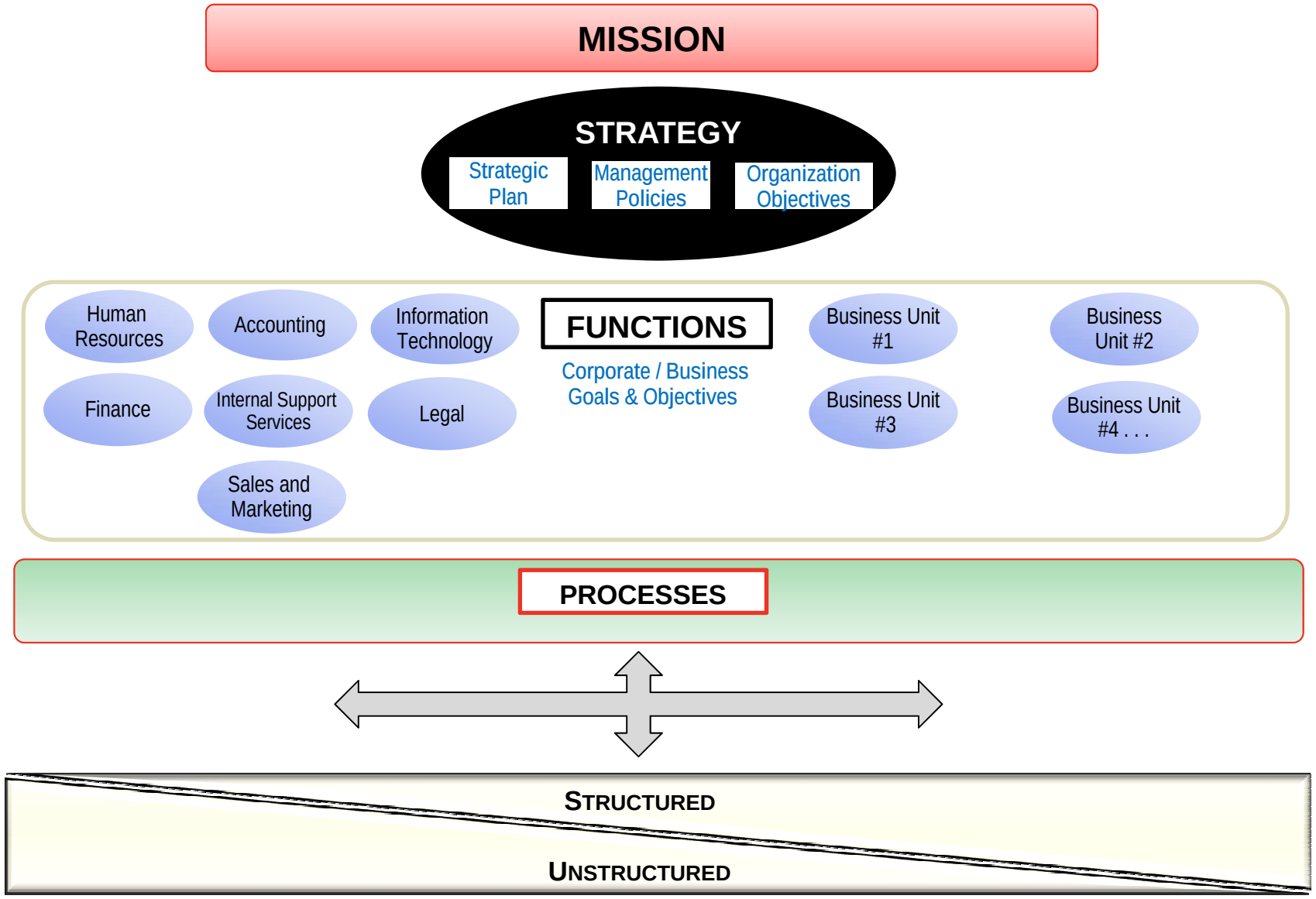
- **Increasing reliance on electronically stored information requires strict controls to properly protect the corporation's intellectual property**

Recent Industry Findings

- "In the records retention area, 31% of all the companies in the survey now log or retain instant messages, and 40% retain voice mail."[1]
- "…suits with $20M or more at stake are on the rise. All of the smallest and mid-sized company respondents reported at least one lawsuit of that magnitude in the past year. Twenty percent of the largest companies surveyed had 21-50 lawsuits of that size…40% of the largest companies surveyed spent US$5 million or more annually on legal fees and disbursements..."[1]
- "According to the study…by the Ponemon Institute, data breach incidents cost companies $197 per compromised customer record in 2007…The average per-incident [cost was] $6.3 million…lost business [cost] increased by 30 percent to an average of $4.1 million…Breaches by third-party organizations such as outsourcers [and] contractors…were reported by 40 percent of survey respondents."[2]
- "Daimler's [Daimler Chrysler] chairman recently admitted he made a mistake by freezing the situation for a year rather than start integrating right away… Communication is essential to integration…How do you share information, how frequently, and with whom?... Macrovision…acquired another software company, InstallShield, several years ago…Macro made sure everyone was informed about everything…Macro kept over 90 percent [of the workforce]."[3]

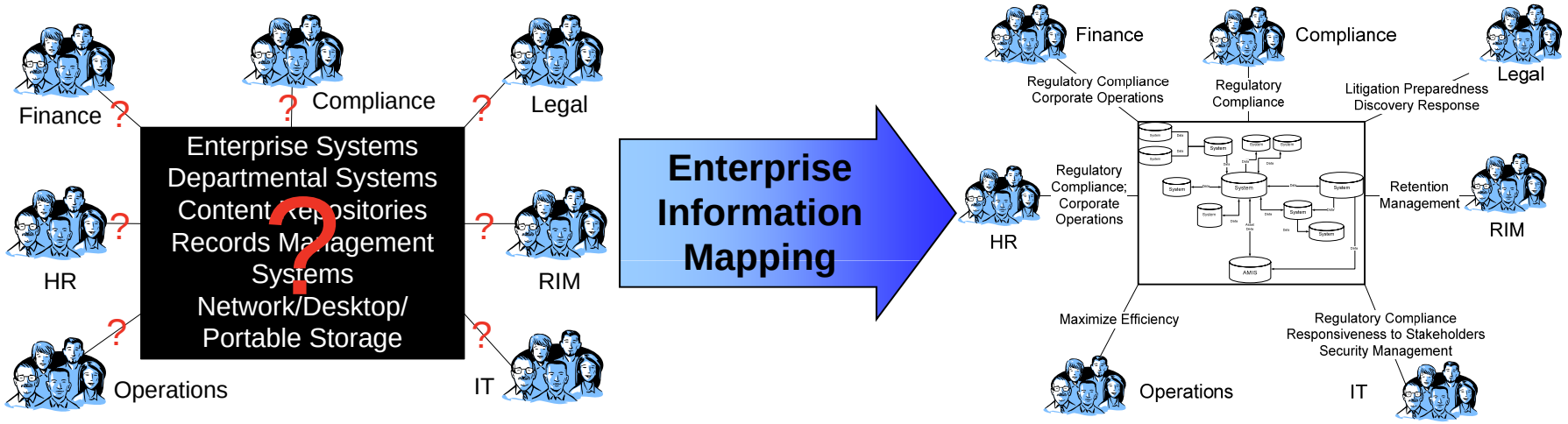
1 Fulbright and Jaworski, LLP, 2007 Litigation Trends Survey
2 "The Costs of Data Breaches Continues to Rise, Says Ponemon" Published: December 10, 2007 by Dan Burger (http://www.itjungle.com/tfh/tfh121007-story08.html)
3 Q&A with Timothy J. Galpin, a senior fellow at Katzenbach Partners LLC (http://www.maadvisor.net/maalerts/08-03-07/alert_main8-3-07.html)

Linking business processes to the information that supports them leads to reduced costs, reduced risk and increased efficiency



We recommend the Enterprise Information Map as a key first step in improving the information management capabilities of an organization

- The enterprise information map provides a comprehensive view of the information systems containing electronically stored information and how they interact

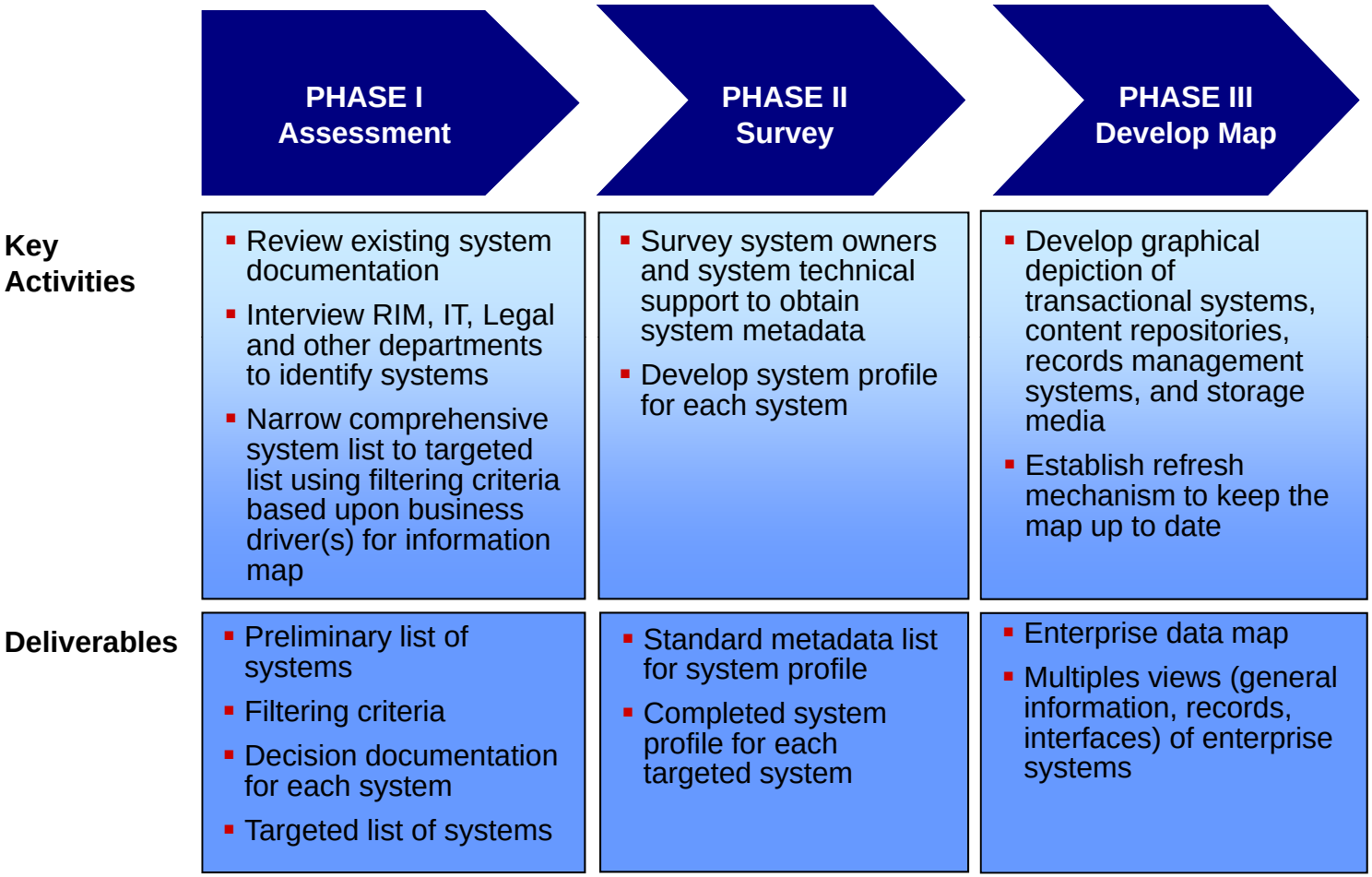


- The enterprise information map is the cornerstone in addressing business pressures and represents a critical step for integrating the electronically stored information within your organization into a comprehensive records and information management program

The EIM meets many needs and supports multiple organizational goals

- **Litigation Preparedness:** Determine systems most likely to be involved in litigation and/or eDiscovery
- **Disaster Recovery:** Determine system priority from a disaster recovery perspective
- **Regulatory Compliance:** Determine systems most likely to include data with regulatory implications/requirements
- **Systems Modernization**: Determine highest priority systems to include record keeping functionality
- **Enterprise Architecture Management:** Facilitate buy –vs- build- vs- leverage decisionmaking process
- **Data Use/Loss Prevention:** Determine systems which pose the highest risk should data loss/breach occur

The Enterprise Information Map provides a snapshot of corporate information repositories and builds a plan for maintaining the map over time



The prioritization of the systems is based on a specific driver

Screening Questions \ EIM Driver	Litigation Preparedness	Disaster Recovery	Regulatory Compliance	Systems Modernization	Enterprise Architecture Management	Data Use/Loss Prevention
1) What business functions does the system support?	1	2	2	1	1	2
2) What types of data and/or documents are housed in the system?	1	1	1	1	1	2
3) Is systems documentation (requirements, design & testing) available?	1	1	1	1	1	1
4) Does the system share information with other systems (if so which)?	1	2	1	2	1	2
5) How many times has the system been affected by a legal hold and/or eDiscovery request over the last 3 years?	2	1	1	1	1	1

- Weighting factors applied to each question are used to reflect the organization's priorities and can be manipulated over time as priorities change

CASE STUDY: Duff & Phelps was engaged to develop a systems modernization roadmap focused on backoffice recordkeeping systems

Goals

- Complete a system inventory of selected key recordkeeping systems and identify which require updates
- Develop systems modernization roadmap to determine the timing for incorporating recordkeeping requirements
- Identify issues to be addressed in electronic records infrastructure
- Gain visibility into data contained in back office systems
- Formalize process for prioritizing new systems as a result of M&A activity

Approach

- Identify preliminary list of systems through discussion with Corporate Technologies
- Identify the sub-set of systems most likely to contain records
- Develop a formal methodology for prioritizing systems
- Develop system profile template for gathering information on each system to feed ranking criteria
- Interview system owners and technical support staff to gather system information
- Develop enterprise data map and system modernization roadmap for selected systems through analysis of system rankings

Findings

- Proprietary findings were provided to the client

PHASE I
Assessment

PHASE II
Survey

PHASE III
Develop Map

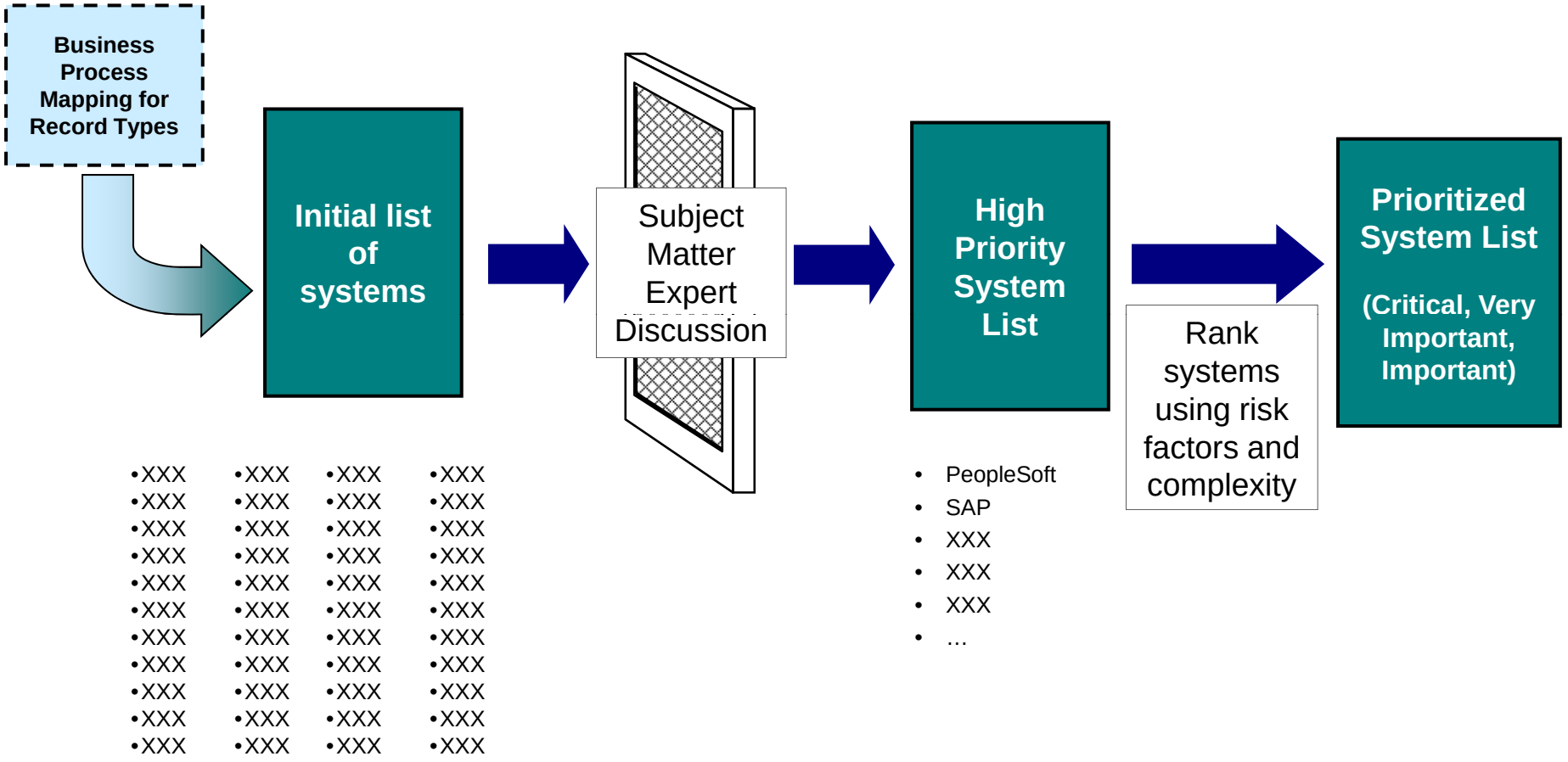
We identified a manageable number of high-level recordkeeping requirements for inclusion in business applications

- **Recordkeeping functionality is generally divided into two major capabilities:**
  1. The capability to make data uneditable by any user through either the user interface, data interfaces, or direct database access, in response to a hold order placed on data within the system (i.e., an entire contract put on a hold for a dispute).
  2. The capability to permanently delete data (i.e., all records for a specific contract) once a certain amount of time has passed, or a certain event has occurred. The time period and event would be specified by an approved records retention schedule.

- **These two capabilities can be further expanded into the following requirements*:**
  1. The System shall prevent the deletion of an electronic file or any part of its contents at all times, except when destruction is in accordance with a retention schedule or the object is deleted by an Administrator as part of an audited procedure.
  2. Whenever the System transfers or exports records, it shall include a copy of all the audit trail data associated with the records, volumes and files being transferred.
  3. The System shall support retention and disposition rules that can be applied at any hierarchical level, with an Administrator-override function.
  4. The System shall support and allow the system administrator to place multiple “legal holds” on each record such that the existence of any single hold will remove that record from the disposition process.
  5. The System shall provide auditing for all user transactions.
  6. The System shall support chronological and event-based retention types.
  7. The System shall provide notification of records eligible for disposition.
  8. The System shall provide a function that specifies retention schedules, automates reporting and destruction actions, and provides integrated facilities for exporting records and metadata.
  9. The System shall automatically record and report all disposition actions to the Administrator.
  10. The System shall permit the association of a retention schedule with any record, file or class of a classification scheme.

* High-level requirements; a more granular decomposition is required for systems design, development and testing

A formal methodology was used to target those systems perceived as high risk for recordkeeping compliance



Through discussions with key stakeholders, we derived a short list of key systems for further study

Previous Phase

Current Phase

For each system on the High Priority List, we worked with business system owners and IT system administrators to develop a detailed system profile

	Risk Factor	System Lifecycle / Size	Other	Total Score
1. AAA	**64***	**21**	**0**	**85**

AAA is an off-the-shelf product sold by XXX Corp. This instance of AAA includes the 111 and 222 modules. The recent implementation has expanded the user community for AAA significantly.

System Profile Summary

- 9 records retention schedules mapped to dataset(s) within system
- $XXX (estimated) spent to-date
- Large user community
- Multiple user interfaces for adding/modifying data
- Large number of interfaces with other systems

Records Retention Schedules

- XXX
- YYY
- ZZZ

System Profile

System Scorecard

Current recordkeeping functionality

- The system tracks an audit log for updates made to data within the system.
- Access controls at the user level can be used to restrict access to specific datasets.

** Scores are driven by the answers are derived based on the answers to the questions on the following pages*

The ‘Risk Factor’ measures the type and volume of records stored in each system

This dimension consisted of fourteen (14)[1] data points addresses the data the system contains, whether the system is the authoritative source for the data, and how the system is managed.

(overall ranking)	Risk Factor
1. AAA (1)	64
2. BBB (2)	48
3. CCC (3)	44
4. EEE (5)	30
5. FFF (6)	30
6. DDD (4)	28
7. GGG (7)	22
8. HHH (8)	16
9. III (9)	14
10. JJJ (10)	14
11. KKK (11)	0

- **AAA maintain data that maps to a significant number of established records retention schedules. Additionally, each of these systems has a large community of users and feeds data to additional systems.**
- **EEE maintain a small number of critical data sets that map to established records retention schedules. FFF and DDD are critical systems to FFF staff responsible for procuring goods and services. EEE is critical to the operations group responsible for frontoffice and backoffice systems at headquarters.**
- **GGG contains critical project management information and shares record data with both FFF and DDD. HHH is the system of record for system development documentation. III is the primary system for generating accounts payable entries for partner settlements and interacts heavily with EEE.**

[1] **Please refer to Appendix A for additional detail on the ranking criteria.**

Ranking Criteria Details – Risk Factor

The total score for all 14 risk factors was multiplied by two (2) to emphasize a risk-based approach to the modernization roadmap and reflect the importance of prioritizing those systems that contain a larger number of official corporate records.

Criterion	Notes	Valid Values	Multiplier
The data (or a subset of the data) stored by the system is currently involved in a legal hold, or other litigation-related activities.	The implication of this criterion is that a system is considered the authoritative source for the data it contains.	Yes / No	2
The data (or a subset of the data) stored by the system is more likely than others to be involved in a future legal hold, or other litigation or investigation related activities based solely on the nature of the content.		Yes / No	1
The system stores personally identifiable information (PII).	Examples include social security number, and home address	Yes / No	1
The system stores data subject to protection under privacy laws.		Yes / No	1
The system stores sensitive financial data.	Examples include P&L data reported to the SEC.	Yes / No	1
The system stores personal credit card information data.		Yes / No	1
Partners or customers utilize the data within the system.		Yes / No	2

Ranking Criteria Details – Risk Factor

Criterion	Notes	Valid Values	Multiplier
The number of users that have accessed the system in the past 12 months.		Less than 100: 1 100-500: 2 Greater than 500: 3	1
The data within the system is used by wholly-owned subsidiaries or affiliates.		Yes / No	2
The system houses global operations data.	Examples of global operations data include human resources data for staff outside the US, financial transactions for business units in countries outside of the US.	Yes / No	1
The system is considered the authoritative source for data that maps to X existing record types with legal requirements.		1 point per record type. Additional point for record types with legal requirements.	1
The system is the primary location for finding the data it contains.	This criterion is focused on identifying whether the system is supported by a paper process, or the data within the system resides in other systems.	Yes / No	2
The current system backup procedures are not managed by a well-defined process.	The assumption is that systems with poorly defined backup procedures receive higher importance.	Yes / No	1
The system allows the data it contains to be modified, either through updates of existing data or addition of new data.	This criterion seeks to measure the complexity of enabling disposition or hold functionality by quantifying whether a moment in time would need to be re-created or if all of the data is available elsewhere..	Yes / No	2

The 'System Lifecycle/Size' dimension measures the size of each system and the degree to which it interacts with other systems

This dimension consists of nine (9)[1] data points addressing the production status of the system, the computing infrastructure supporting the system, the costs spent to-date on the system, and the system and user interfaces for moving data into and out of the system.

(overall ranking)	System Lifecycle / Size
1. AAA (1)	21
2. CCC (3)	16
3. III (9)	16
4. EEE (5)	14
5. BBB (2)	13
6. DDD (4)	13
7. GGG (7)	13
8. FFF (6)	12
9. HHH (8)	11
10. JJJ (10)	9
11. KKK (11)	0

- These are large, expensive systems that have many users and system interfaces for entering/exchanging data. AAA also has a large number of user interfaces for entering data, and exchanges data with both CCC and BBB.
- EEE has a small number of interfaces, but shares contract data with other systems and is a significant investment. BBB and DDD both have a large number of system interfaces.
- GGG has a small number of users and system interfaces, but represents a significant investment. FFF shares critical contract data and interfaces with GGG. HHH has a small number of users and system interfaces, but shares critical accounts payable data with BBB.

[1] Please refer to Appendix A for additional detail on the ranking criteria.

Ranking Criteria Details – System Lifecycle / Size

Criterion	Notes	Valid Value	Multiplier
The system is currently deployed in production and data is actively being added to the system.		Yes / No	2
The estimated total cost spent to date on the system.	For purchased systems, the purchase price (including professional services) as well as maintenance costs paid to-date should be included.	Less than $1M : 1 $1M - $2.5M: 2 Over $2.5M: 3	1
The most recent release of the system into production was within the last 12 months, or the system was moved into production within the last 12 months.	The implication is that systems that are being updated or moved into production will have a longer operational life than those that are stagnant.	Yes / No	1
The system is scheduled to be decommissioned within the next 12 months.	The implication is that systems that are scheduled for decommission imply less risk. The assumption is that the data from the system is being subsumed by another system, or that the data is being archived.	Yes = 0; No = 1	1
The number of user interfaces that enable data to be extracted from the system.		#	2 * number of user interfaces

Ranking Criteria Details – System Lifecycle / Size

Criterion	Notes	Valid Value	Multiplier
The number of systems that send data to or receive data from the system.		Less than 5: 1 5-10: 2 More than 10: 3	1
The total amount of high tier storage currently in use.	1 TB = ~$90K annually (cost) 5 TB = ~$450K annually (cost)	None: 0 Less than 1TB: 1 1TB – 5TB: 2 More than 5TB: 3	2
The total amount of low tier (includes bulk, low, and mid-level) storage currently in use.	2 TB (mid-tier) = ~$100K annually (cost) 9TB = ~$460K annually (cost)	Less than 2TB: 1 2 TB-9TB: 2 More than 9TB: 3	1
The total number of rows of data in the system.		Less than 1M: 1 1M – 5M: 2 More than 5M: 3	1

The 'Other' dimension measures the flexibility that the organization has to modify each system to meet recordkeeping requirements.

This dimension consists of two (2)[1] data points addressing whether the system is an off-the-shelf product with an active maintenance contract, or a system developed by XXX.

(overall ranking)	Other
1. DDD (4)	4
2. HHH (8)	4
3. GGG (7)	2
4. AAA (1)	0
5. BBB (2)	0
6. CCC (3)	0
7. FFF (6)	0
8. EEE (5)	0
9. III (9)	0
10. JJJ (10)	0
11. KKK (11)	0

- YYY was built by XXX and is currently maintained by XXX employees. AAA application was built by XXX employees and is currently maintained by XXX employees. YYY application is a COTS-based application that was customized for XXX and does not have an active maintenance contract.
- The remaining systems are off-the-shelf products that have an active maintenance contract.

[1] Please refer to Appendix A for additional detail on the ranking criteria.

Ranking Criteria Details – Other

The total score for the 2 other criteria was multiplied by two (2) to incorporate the difficulty in modifying an unsupported application, or identifying internal staff to perform system maintenance in addition to their regular duties.

Criterion	Notes	Valid Value	Multiplier
The system is a Commercial-off-the-Shelf (COTS) product that is no longer supported through a maintenance contract with a vendor.		Yes / No	1
The system is an internally developed product or system.		Yes / No	2

Based on the aggregate scores, we divided the systems into three categories of priority for remediation

	Risk Factor	System Lifecycle / Size	Other	Total Score
1. AAA	64	21	0	85
2. BBB	48	13	0	61
3. CCC	44	16	0	60
4. DDD	28	13	4	45
5. EEE	30	14	0	44
6. FFF	30	12	0	42
7. GGG	22	13	2	37
8. HHH	16	11	4	31
9. III	14	16	0	30
10. JJJ	14	9	0	23
11. KKK*	0	0	0	0

Critical (Total score >=60)

- This group contains systems with the highest overall score, indicating that the system is considered a high priority to modernize to support records keeping functionality

Very Important (Total score >40 and <60)

- This group contains systems with a high overall score, indicating that the system is considered a moderate priority to modernize to support records keeping functionality

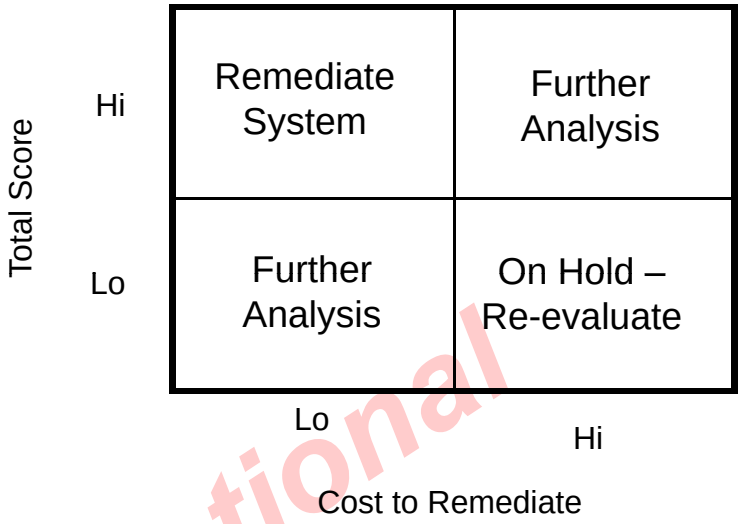
Important (Overall score >30 and <40)

- This group contains systems with a lower overall score, indicating that the system is considered a lower priority to modernize to support records keeping functionality

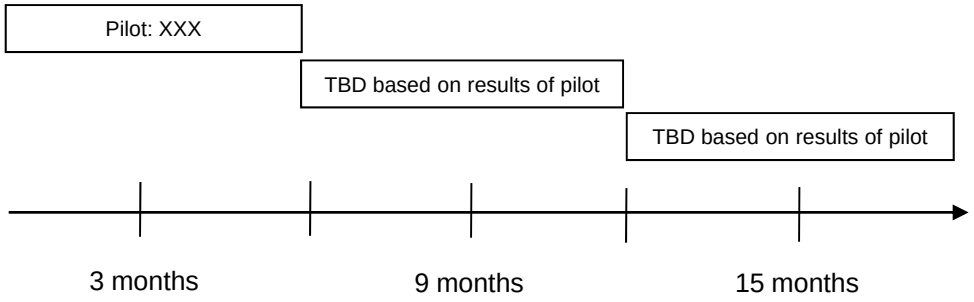
*** We were unable to obtain visibility into this system during this evaluation.**

We then followed a formal methodology to develop the sequencing plan for remediation

- **Accurate risk and cost data informs the decision on addressing remediation**

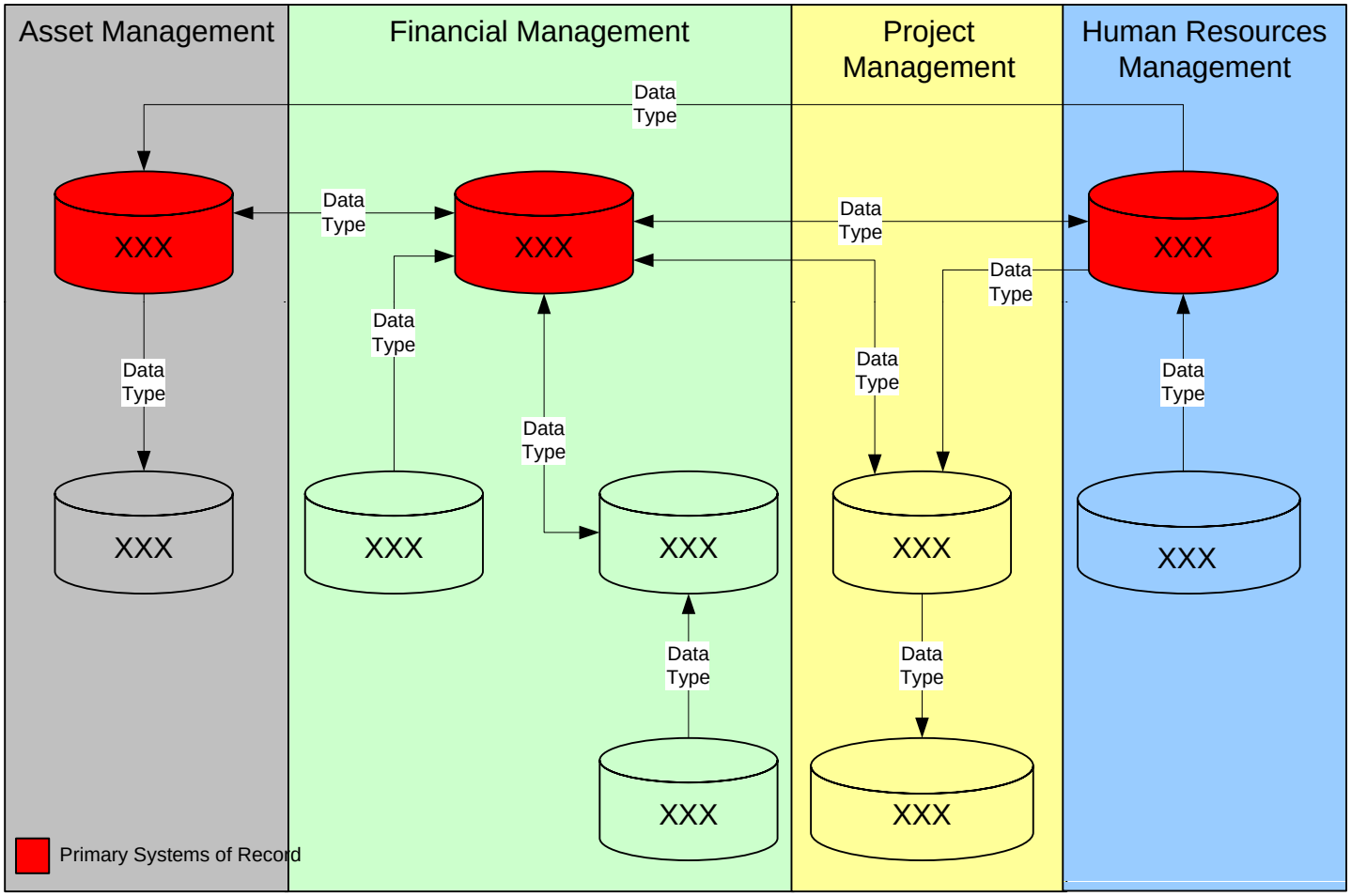


- **The sequence for addressing priority systems will be driven by this analysis**

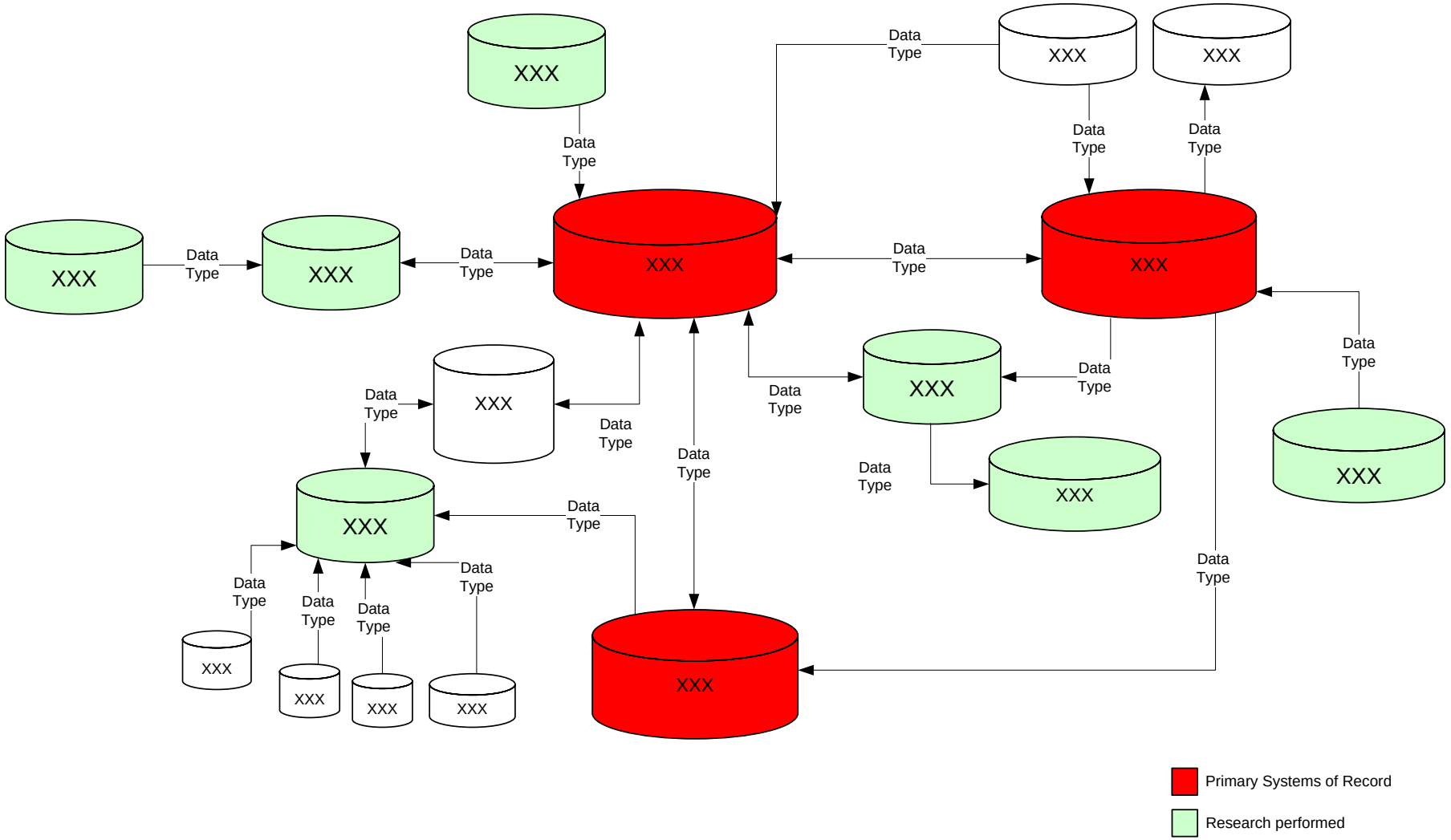


	Total Score	Estimated Cost to Remediate
1. AAA	85	TBD
2. BBB	61	~$20K
3. CCC	60	TBD
4. DDD	45	~$25K
5. EEE	44	~$180K
6. FFF	42	~$160K
7. GGG	37	TBD
8. HHH	31	TBD
9. III	30	TBD
10. JJJ	23	TBD
11. KKK	0	N/A

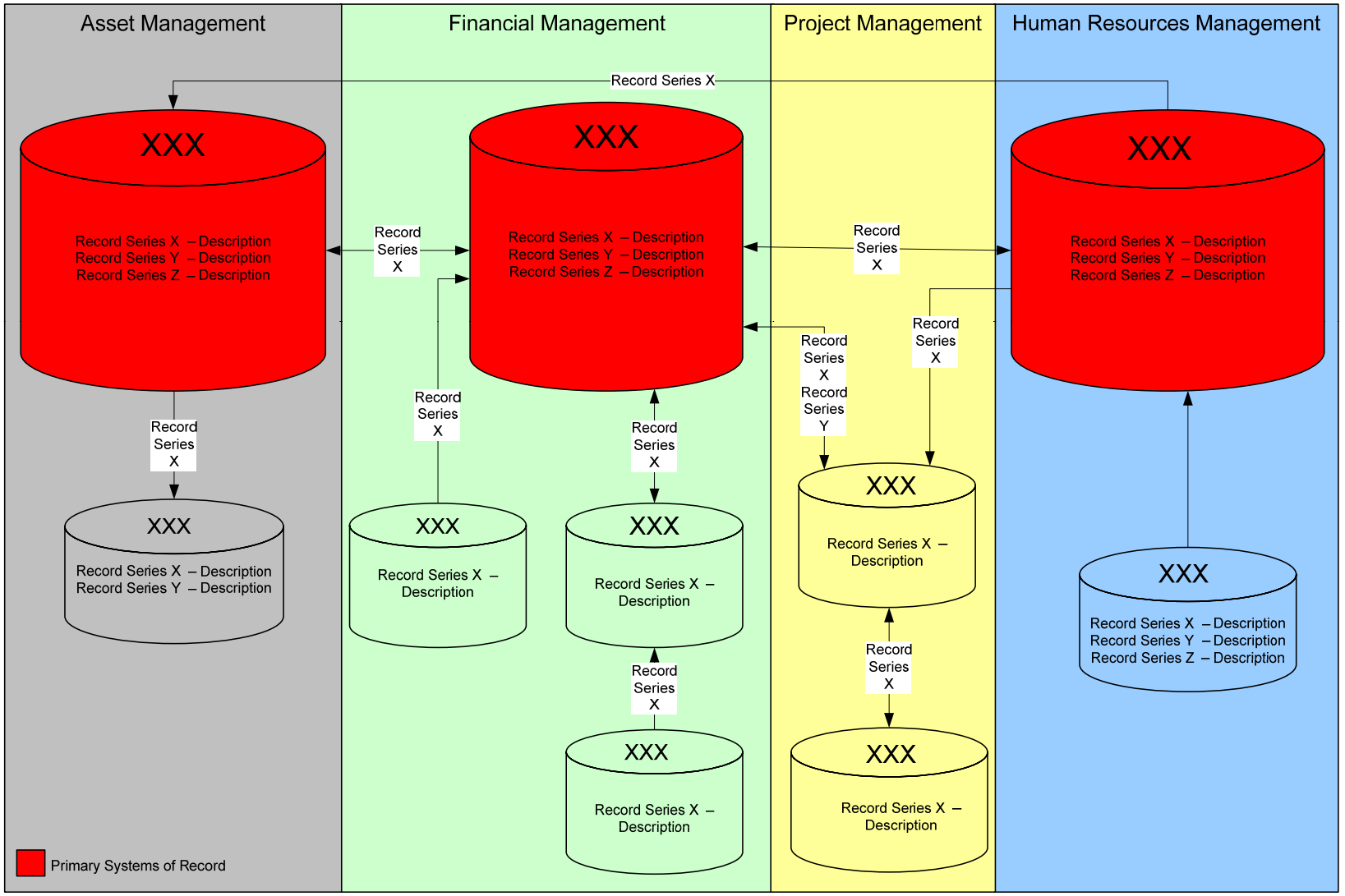
We provided the client with a number of views into their systems: *High Level Enterprise Data Map (Information View)*



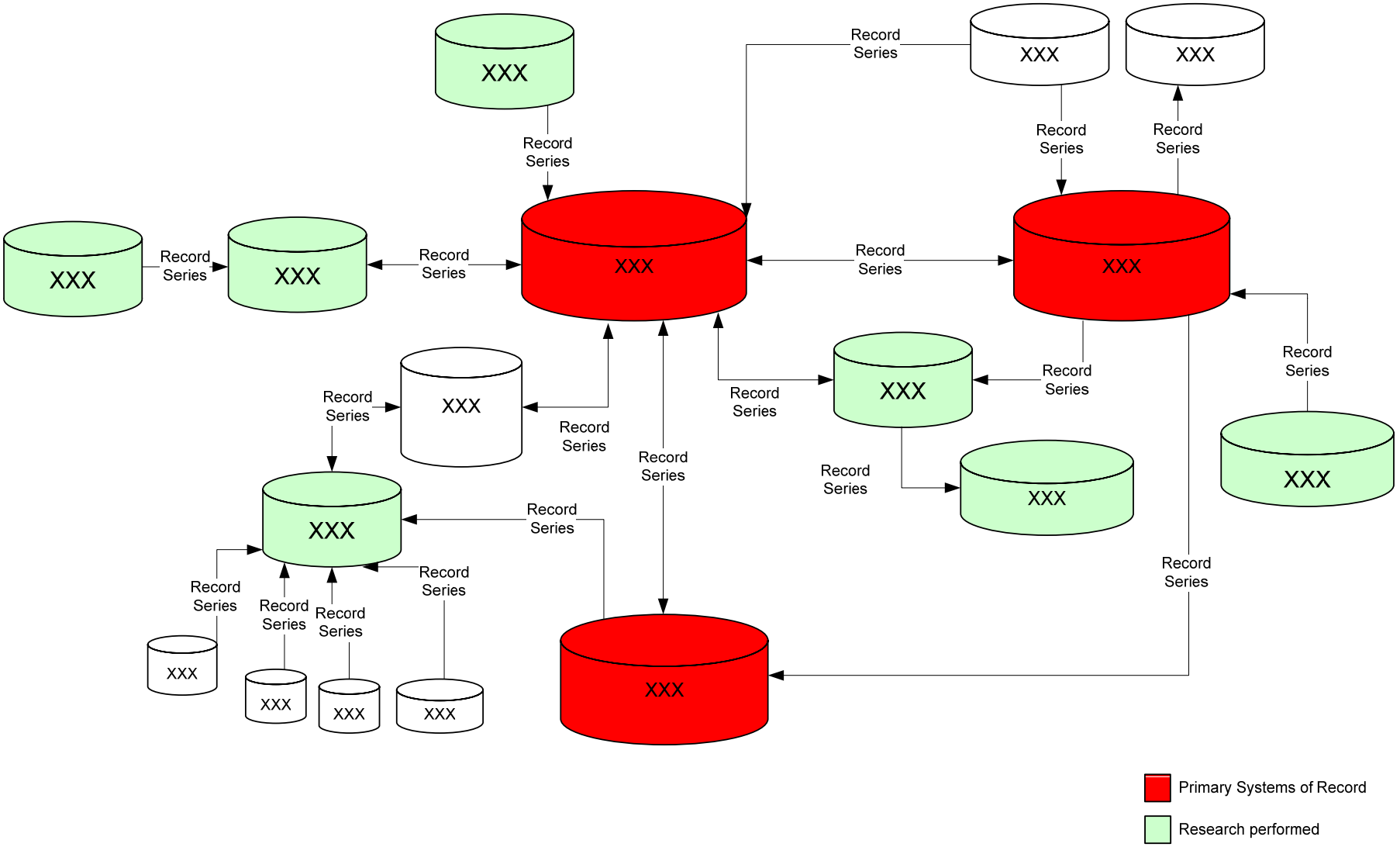
Detailed Enterprise Data Map (Information View)



High Level Enterprise Data Map (Record View)



Detailed Enterprise Data Map (Record View)



Contact

Maura L. Dunn, CRM, PMP

Director, Legal Management Consulting

Duff & Phelps, LLC

240.482.3982

maura.dunn@duffandphelps.com