UNITED STATES
OFFICE OF PERSONNEL MANAGEMENT

HUMAN RESOURCES LINE OF BUSINESS

TECHNICAL MODEL VERSION 1

January 2008

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

Foreword to HR LOB Technical Model (TM) version 1

The Human Resources Line of Business (HR LOB) initiative was launched in 2004 to support the vision articulated in the President's Management Agenda. The HR LOB is expected to help the Federal Government realize the potential of electronic government by significantly enhancing human resources service delivery within the Executive Branch. The HR LOB Concept of Operations (CONOPS) proposes a near-term Service Delivery Model where HR services relating to human resources information systems (HRIS) and payroll operations move from the agencies to HR shared service centers. Over time, as HR shared service centers evolve and expand their capabilities, more transactional and administrative activities may shift from the agency to the service center delivery mode. The HR LOB approach will allow agencies to increase their focus on core mission activities and the strategic management of human capital, while HR shared service centers deliver the HR services defined in the HR LOB CONOPS in an efficient and cost-effective manner with a focus on customer service and quality.

This document addresses the HR LOB Technical Model (TM) for the core HR LOB sub-functions – Compensation Management and Benefits Management – and those activities that result in a Personnel Action. In accordance with OMB's Federal Enterprise Architecture guidance, the Technical Model (TM) outlines the standards, specifications, and technologies that collectively support the secure delivery, exchange, and construction of business and application components (Service Components) that may be used and leveraged in a Component-Based or Service Orientated Architecture. The TM identifies the core technologies for the HR LOB core sub-functions that support the Federal Government information technology (IT) transition towards interoperable e-Government solutions.

The Technical Model (TM) is an integral component of the HR LOB enterprise architecture and is required by the Office of Management and Budget (OMB) as part of a Federal Information Technology Architecture (OMB M-97-16). The purpose of the HR LOB TM is to provide a common technical vocabulary so agencies and the HR LOB shared service centers can efficiently coordinate acquisition, development, implementation, and support of HR LOB's information systems.

Human Resources Line of Business
Technical Model (TM)
Version 1

Table of Contents

List of Figures

1.0 Introduction

Enterprise architectures provide a basis for understanding commonalties across business entities and an opportunity for collaboration and sharing. The Federal Enterprise Architecture is comprised of five reference models. Collectively, the models provide universal definitions and constructs of the business, performance and technology of the Federal Government. The reference models will serve as a foundation to leverage existing processes, capabilities, components and technologies as future investments are made. They are designed to provide a governmentwide view that will help identify duplicative investments and opportunities for collaboration within and across Federal agencies. Figure 1 – Federal Enterprise Architecture (FEA) Reference Models shows this collection of interrelated "reference models".

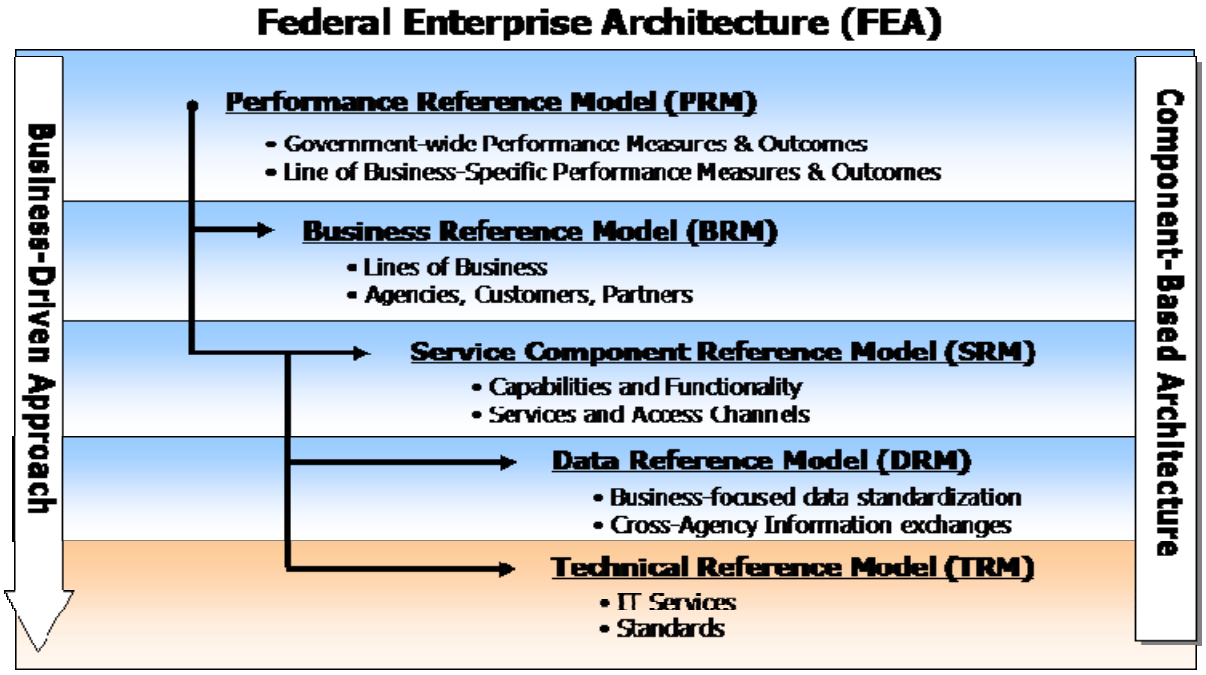


Figure 1 -- FEA Reference Models Hierarchy

The Human Resources Line of Business Technical Model (TM) is a conceptual framework providing the following: A consistent set of service and interface categories and relationships used to address interoperability and open-system issues; conceptual entities that establish a common vocabulary to better describe, compare, and contrast systems and components; a basis (an aid) for the identification, comparison, and selection of existing and emerging standards and their relationships. It is not a specific system or solution design. Rather it establishes a common vocabulary and defines a set of services and interfaces common to the solutions. The associated standards profile identifies standards and guidelines in terms of the reference model services and interfaces. These standards and guidelines can be applied and tailored to meet specific agency or Shared Service Center (SSC) requirements. By design, the HR LOB Technical Model will

facilitate analysis of requirements, architecture, design, implementation, and testing of heterogeneous systems.

The first version of the HR LOB Technical Model (TM) focuses on the core Business Reference Model (BRM) sub-functions -- Compensation Management and Benefits Management -- and those BRM activities that result in a Personnel Action. It will be expanded over the next several months to include service components for the remaining Business Reference Model sub-functions.

1.1 HR LOB Background

The HR Line of Business will help the Federal Government realize the potential of electronic government and redefine human resources service delivery for civilian employees of the Executive Branch. The HR LOB Concept of Operations (CONOPS) proposes a near-term approach to shared services where HR services relating to human resources information systems (HRIS) and payroll operations move from the agencies to HR shared service centers. Over the longer term, additional services may be moved from agency HR operations to service providers. The Service Component Model provides a framework and vocabulary for guiding discussions between providers and customer agencies. It identifies basic HR services – service components – and proposes the best provider/customer delivery channel for each service – Service Delivery Model.

The HR LOB objectives and goals will be the key to evaluating the success of this new HR service delivery approach. The intended results of this new delivery model are:

- improved management of human capital throughout the Federal Government
- increased operational efficiency
- lower costs
- better customer service

1.2 HR LOB Enterprise Architecture

The HR service delivery approach proposed by the HR LOB is a new model for doing business in the Federal Government. The breadth of this initiative spans Human Resources for the Executive Branch civilian labor force. To help manage the complexity of this effort, a set of architectural blueprints is being constructed to provide a common picture and a common vocabulary for the business of HR in the Federal Government.

Five models comprise the HR LOB Enterprise Architecture (EA). OMB's Federal Enterprise Architecture (FEA) standards guide their development:

- Performance Model: "…a framework for performance measurement providing common output measurements throughout the Federal Government. The model articulates the linkage between internal business components and the achievement of business and customer-centric outputs."

- Business Reference Model: "…a framework that facilitates a functional (rather than organizational) view of the Federal Government's lines of business, including its internal operations and its services for citizens, independent of the agencies, bureaus and offices that perform them. The BRM describes the Federal Government around common business areas instead of through a stove-piped, agency-by-agency view."

- Service Component Model: "…a business-driven, functional framework classifying Service Components according to how they support business and performance objectives. Its serves to identify and classify horizontal and vertical Service Components supporting Federal agencies and their IT investments and assets."

- Data Model: "…is intended to promote the common identification, use and appropriate sharing of data/information across the Federal Government through its standardization of data in the following three areas: data context, data sharing and data description."

- Technical Model: "…a component-driven, technical framework that categorizes the standards and technologies to enable and support the delivery of Service Components and capabilities. It also unifies existing agency technical models and E-Gov guidance by providing a foundation to advance the reuse and standardization of technology and Service Components from a governmentwide perspective."

Collectively, the five models provide a comprehensive view of how a Federal enterprise's business mission is supported or enabled by processes, information, organization and underlying information systems and technologies.

Four of the five models have been published:

- BRM version 2 – The BRM is an end-to-end process view of human resources for the Executive Branch of the U.S. Federal Government. BRM version 1 was published in December, 2004. During the fall of 2005, 47 HR subject matter experts representing 14 Federal agencies reviewed and refined the previous BRM and recommended a revised BRM consisting of 45 processes organized into 10 sub-functions. Each of these processes is further decomposed to the activity level definitions. (Report can be viewed at http://www.opm.gov/egov/documents/architecture/#brm)

- Data Model version 1 – Completed in January 2006, the Data Model describes two different views – a Conceptual Data Model (CDM) and the Logical Data Model (LDM). The CDM is a single integrated data structure that shows data objects along with high-level relationships among data objects. The LDM includes more detail for a subset of the CDM scope: The data to be shared across agencies and SSCs. It shows data entities, attributes and relationships between entities. (Report can be viewed at http://www.opm.gov/egov/documents/architecture/#drm)

- Performance Model version 1 for core business areas constitutes publication addressing the third architectural component, the PRM. The HR LOB PM proposes a common set of performance measures for use throughout the Federal Government. These performance

measures will gauge how effectively government HR resources are used to support agency mission results, support the effective management of human capital across the government and provide for effective human resources service delivery to employees, managers/supervisors and other HR constituents. (Report can be viewed at http://www.opm.gov/egov/documents/architecture/#pm)

- Service Component Model version 2 identifies HR services – *service components* – and proposes the means for providing them to its customers – *service delivery*. It provides a framework and vocabulary for guiding discussions between service providers and customer agencies and is meant to be a catalyst for true cross-agency collaboration. (Report can be viewed at http://www.opm.gov/egov/documents/architecture/#scm)

The HR LOB Service Component Model (SCM) Version 2 defines two concepts that support the objective of the Human Resources Line of Business (LOB). These two concepts are *reusability* and *interoperability*.

- Reusability is the ability to utilize a business asset in more than one context – by multiple organizations or across multiple processes.
- Interoperability is the ability to exchange assets for like assets without undue impact. It enables the consumer of the asset to trade out one piece for another without a big rippling effect. To minimize the ripples, the asset must be self-contained and independent in terms of what it accomplishes and the resources it needs to accomplish it.

The HR LOB Technical Model (TM) along with standards profile and best practices will facilitate the reusability of service components at both business and technical levels and will promote interoperability of technical service components.

1.3 Overview of HR LOB Technical Model (TM)

The HR Line of Business Technical Model (TM) objectives are based on the Federal Enterprise Architecture (FEA) framework published by the Office of Management and Budget (OMB). The FEA is a business-based framework for governmentwide improvements to facilitate efforts to transform the Federal Government into one that is citizen-centered, results-oriented, and market-based.

A technical model is necessary to establish a context for understanding how the disparate technologies required to implement HR LOB solution relate to each other. The model also provides a mechanism for identifying the key issues associated with applications portability, scalability, and interoperability. Without the presence of a technical model, interfaces are based on ad-hoc efforts, leading to rigid information infrastructures, duplicate efforts, the continual reinvention of the wheel, and as many systems with interfaces as potential partners.

The HR LOB Technical Model is a conceptual framework that provides a consistent set of service and interface categories and relationships used to address interoperability and open-system issues; conceptual entities that establish a common vocabulary to better describe, compare, and contrast systems and components; a basis (an aid) for the identification, comparison, and selection of existing and emerging standards and their relationships. It is not a

specific system or solution design. Rather it establishes a common vocabulary and defines a set of services and interfaces common to the solutions. The associated standards profile identifies standards and guidelines in terms of the reference model services and interfaces. These standards and guidelines can be applied and tailored to meet specific agency or SSC requirements. By design, the TM will facilitate analysis of requirements, architecture, design, implementation, and testing of heterogeneous systems.

It is important to understand that though the HR LOB Technical Model defines and describes technical components and services that facilitate service components reuse and interoperability, it does not recommend or endorse any vendor products. It also makes no statements or implications about what organization structure should be put in place to support and exploit the technology, or which individuals should have particular roles, and what processes should be implemented to exploit the technology.

1.4 HR LOB Technical Model Objectives

The goal of the HR LOB Technical Model is to facilitate service components in achieving effective levels of reusability and interoperability in the following ways:

- By providing a consistent and common lexicon for description of interoperability requirements between diverse systems
- By providing a means for consistent specification and comparison of system/service architecture
- By providing support for commonality across systems
- By promoting the consistent use of standards
- By aiding in the comprehensive identification of information exchange and interface requirements

The objectives of the HR LOB Technical Model are:

- **Improve User Productivity:** User productivity improvements will be realized by applying the following principles:
    - Consistent User Interface
    - Service components reuse
    - Data Sharing
- **Improve Development Efficiency**: The efficiency of development efforts will be improved by applying the following principles:
    - Common Development
    - Common Open System Environment
    - Use of Commercial Products
    - Software Reuse
    - Resource Sharing
- **Improve Interoperability**: Interoperability improvements across applications and agency or LOB areas can be realized by applying the following principles:
    - Common Infrastructure
    - Standardization

- **Promote Vendor Independence**: Vendor independence will be promoted by applying the following principles:
    - Interchangeable Components
    - Non-proprietary Specifications
- **Reduce Life Cycle Costs**: Life cycle costs can be reduced by applying most of the principles discussed above. In addition, the following principles directly address reducing life cycle costs:
    - Reduced Duplication
    - Reduced Software Maintenance Costs
    - Reduced Training Costs

1.5 HR LOB Technical Model Guiding Principles

Five primary guiding principles for the Technical Model (TM) are essentially derived from the definition and purpose of the HR LOB and emphasize its different aspects. These principles are:

- Comprehensiveness: Three areas the TM must cover to be comprehensive include; reusable services and interoperability of applications, technologies involved in HR LOB interoperability, and the requirements for describing the human aspects of interoperability.
- Easy to Interpret: The TM should enable users to rapidly interpret its contents and place it within their own context. In addition, the TM must use well-defined terms, must clearly define its terms, and provide examples to enable users to distinguish between distinct but related ideas or concepts.
- Traceability: The TM serves as an architectural foundation; therefore, it must be well documented. By establishing traceability, users can determine whether the TM covers their critical areas of interest.
- Usability: The TM should help end-users and system developers communicate with each other across domain and technology boundaries. This communications bridge spans from end-users to both solution providers and other technical users. The TM should provide descriptive measures of interoperability.
- Independence: By definition, the TM should not be tied to a specific application architecture, design, or implementation. Users and providers must be able to map their application requirements and technologies to the TM regardless of how or when developed.

1.6 Common Terminology and Definition

Technologies – refers to a specific implementation of a standard within the context of a given specification.
Component **-** a self-contained business process or service with predetermined functionality that may be exposed through a business or technology interface.
Service Area – is a technical tier that supports the secure construction, exchange, and delivery of business or service components. Each Service Area groups the requirements of component based architectures within the Federal Government into *functional* areas.
Service Category **–** is a sub-tier of the Service Area to classify lower levels of technologies, standards, and specifications in respect to the business or technology function they serve.

Standard – hardware, software, or specifications widely used and accepted (de facto), or sanctioned by a standards organization (de jure).

1.7 Structure of the Document

The document is organized according to the following chapters:

***Chapter* 1** introduces the HR LOB Technical Model and defines its objectives.
***Chapter* 2** describes the structure and details of technical services included in the HR LOB Technical Model.
Chapter 3 discusses the Standards Profile (SP), adoption process, and relationship to the HR LOB TM
Chapter 4 discusses the traceability of the Technical Model to the HR LOB Service Components and requirements.
Chapter 5 is an analysis of the HR LOB TM with conclusion and recommendations.
***Appendix* A** contains Delivery Process-Action diagrams for the HR LOB Core service components.
***Appendix* B** contains the traceability matrix showing TM component relationship to the requirements
***Appendix* C** contains the list of abbreviations and acronyms
***Appendix* D** contains the table that lists out standards applicable to service categories described in the HR LOB Technical Model
***Appendix* E** contains the diagram showing the HR LOB Technical Model analogy to the "Building Construction Code"

1.8 Audience and Intended Use

The HR LOB Technical Model is intended for use by IT managers, procurement officials, program and project sponsors, technical and systems architects, software developers and maintainers, security architects, systems integrators, vendors, service providers, and supporting contractors.

It will provide guidance in:

- Understanding the existing and emerging HR LOB IT infrastructure and application development environment; and in
- Acquiring, developing and deploying systems consistent with that infrastructure and environment.

The HR LOB TM is intended to support three principal uses in conjunction with standards profiles:

- Ensuring interoperability among HR LOB application systems and with external systems and users,
- Guiding the design of system and technical architectures, and
- Providing the basis for assessing architectural compliance for technical solutions.

Interoperability is the primary concern at the HR LOB. This TM incorporates the elements of the Federal Enterprise Architecture (FEA) TRM to ensure interoperability with external and internal users of HR LOB provided Service Components as well as with the service components external to the HR LOB. This TM provides a technology-focused, vendor-independent view of the hardware and software services that will support the HR Line of Business.

2.0 Structure of the HR LOB Technical Model

The HR LOB Technical Model (TM) is a component-driven, technical framework used to identify the standards, specifications, and technologies that support and enable the delivery of service components and capabilities. The HR LOB TM structure is intended to reflect the separation of data from applications, and applications from the computing platform -- a key principle in achieving open systems. Interoperability is dependent on the establishment of a common set of services and interfaces system developers can use to resolve technical architectures and related issues.

The Federal Enterprise Architecture Technical Reference Model (FEA TRM) provides a foundation to describe the standards, specifications, and technologies to support the construction, delivery, and exchange of business and application components (Service Components) that may be used and leveraged in a Component-Based or Service-Orientated Architecture.

2.1 TM Structure Overview

The HR LOB TM has adopted the three level hierarchical structure defined by the FEA TRM:

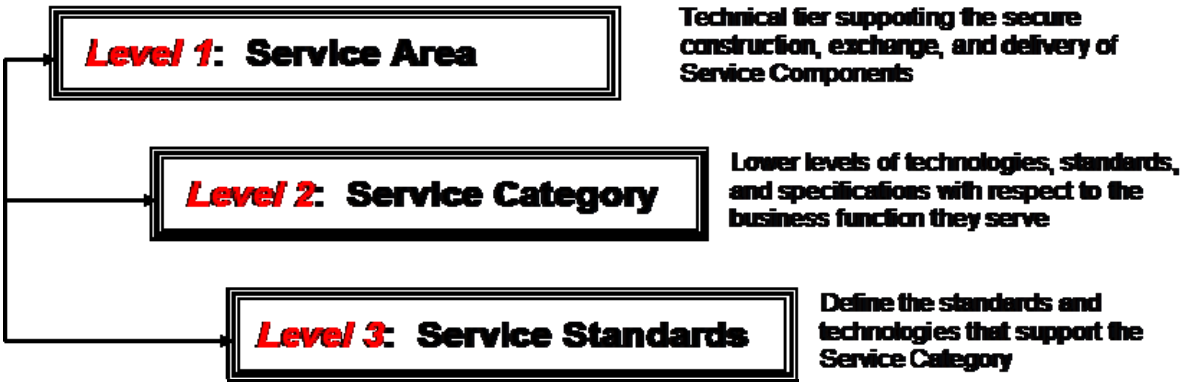


Figure 2 -- FEA TRM Structure

- **Service Area** – Defines a technical tier that supports the secure construction, exchange, and delivery of business or service components. Each Service Area groups the requirements of component based architectures within the Federal Government into functional areas
- **Service Category** – Defines sub-tier of the Service Area to classify lower levels of technologies, standards, and specifications in respect to the business or technology function they serve
- **Service Standard** – Defines the standards and technologies that support the Service Category, or hardware, software, or specifications that are widely used and accepted.

The FEA TRM provides a view of technical services, protocols and interfaces that are primarily concerned with supporting the implementation of *Service Components*, as defined in the FEA Service Reference Model (SRM).

2.2 TM Structure Description

The HR LOB Technical Model is organized into five (5) core Service Areas, each with supporting service categories, and each service category with supporting standards. The HR LOB Technical Model aligns very closely to the FEA TRM. In fact, HR LOB Technical Model uses the FEA TRM as the basis starter set and extends the FEA TRM by defining an additional Service Area and several additional categories to address the specific requirements of the HR LOB. Each Service Area aggregates and groups the standards, specifications, and technologies into lower-level functional areas. The five (5) Service Areas within the HR LOB Technical Model are:

- ***Service Access and Delivery***— refers to the collection of standards and specifications to support external access, exchange, and delivery of service components or capabilities. This area also includes the Legislative and Regulatory requirements governing the access and usage of the specific service component.

- ***Service Platform & Infrastructure***—refers to the collection of delivery and support platforms, infrastructure capabilities, and hardware requirements to support the construction, maintenance, and availability of a service component or capabilities.

- ***Component Framework***—refers to the underlying foundation, technologies, standards, and specifications by which service components are built, exchanged, and deployed across service–oriented architectures.

- ***Service Interface and Integration***—refers to the collection of technologies, methodologies, standards, and specifications that govern how agencies will interface (internally and externally) with a service component. This area also defines the methods by which components will interface and integrate with back office / legacy assets.

- ***LOB Specific Technical Services*** —refers to the collection of technologies, methodologies, standards, and specifications that support and govern the technical infrastructure in HR LOB. This area also defines the standards by which desktop and core service components will interface and integrate with HR LOB applications.

The following Figure – 3 shows the HR LOB Technical Model structure. The HR LOB Technical Model is based upon the Federal Enterprise Architecture (FEA) Technical Reference Model. FEA TRM has already defined elements that cover the majority (about 80%) of technical service components required for the HR LOB TM. These definitions serve as good starter set. The remaining technical service components and standards for accommodating HR LOB domain-specific requirements (20 %) will be identified via a detailed review and analysis of the *HR LOB Target Requirements for Shared Service Centers*.

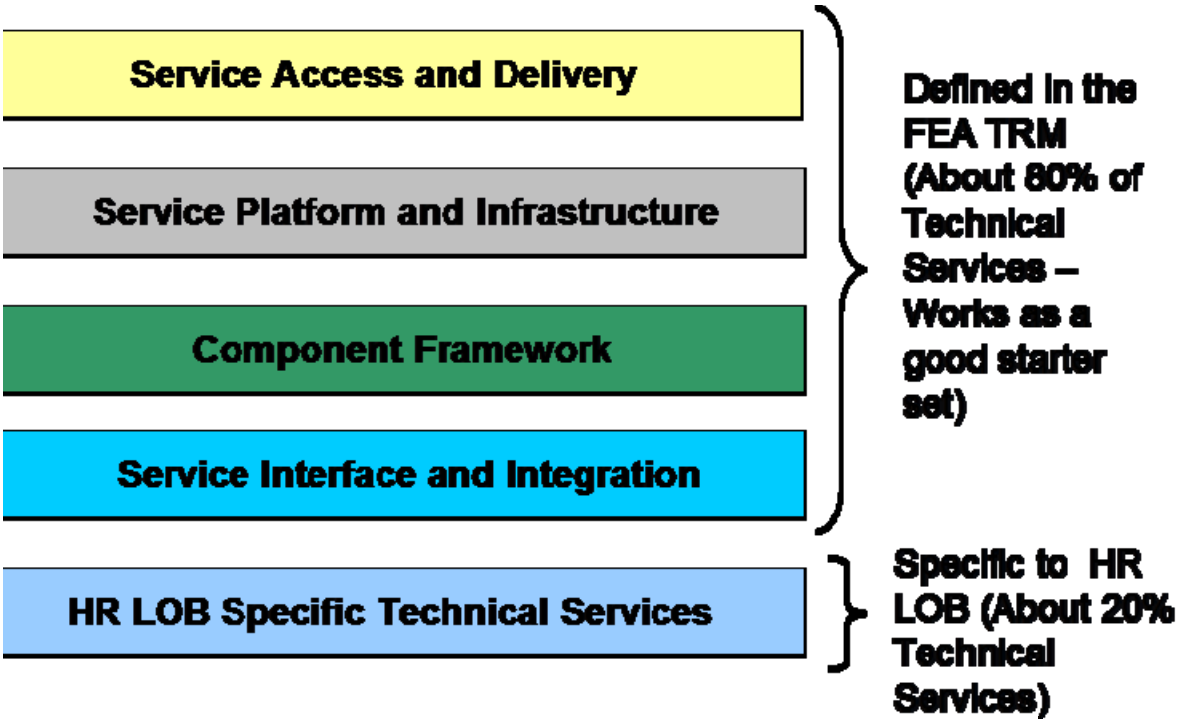


Figure 3 -- HR LOB Technical Model Structure

Each Service Area consists of multiple Service Categories, Service Standards, and Service Specifications that provide the foundation to group standards, specifications, and technologies that directly support the Service Area. Supporting each Service Area is a collection of Service Categories. Service Categories are used to classify lower levels of technologies, standards, and specifications in respect to the business or technology function they serve. Each Service Category is supported by one or more Service Standards. Service Standards are used to define the standards and technologies that support the Service Category.

2.2.1 Service Access and Delivery

The Service Access and Delivery Service Area, as illustrated in Figure - 4, defines the collection of Access and Delivery Channels that will be used to utilize the service component, and the legislative requirements that govern it's use and interaction.

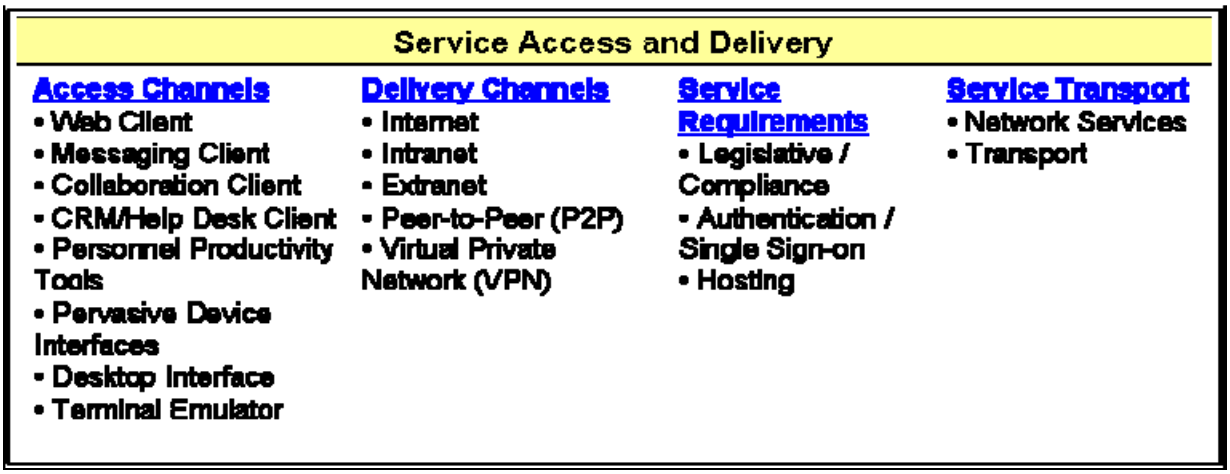


Figure 4 -- Service Categories for "Service Access and Delivery"

Service Categories, Standards, and Specifications for the service area "Service Access and Delivery" are defined below:

Access Channels

Access Channels define the interface between an application and its users, whether it is a browser, personal digital assistant, or other medium.

Web Client – Defines the program that serves as the front end to the World Wide Web (WWW) on the Internet. Web browsers are not just web clients. Popular web browsers also include clients for other Internet services such as FTP and LDAP. Not all web clients are web browsers. A web client can be a specialized program written to provide a limited type of access to resources. A lot of programming languages supply building blocks for making web clients. This means a programmer only has to spend a couple of hours to write one. Specialized web clients are often written in the Java programming language because Java is widely used on the Internet.

Messaging Client – Defines messaging architecture and interface component for applications such as electronic mail, scheduling, calendaring and document management. The messaging client provides a consistent interface for multiple application programs to interact with multiple messaging systems across a variety of hardware platforms. Messaging client software includes applications that run on workstations and enable peer-to-peer, asynchronous communications. The Web Messaging client is constructed to support messaging into standard browsers without specialized plug-ins.

Collaboration Client – Defines the access channel that is designed to help businesses consolidate applications into a single interface including instant messaging, conferencing and traditional telephony. It will allow end users to initiate collaboration sessions directly from their existing desktop applications.

Help Desk Client – Defines the user interface that receives the problems as reported by end users as well as events or alerts generated automatically. The help desk client will receive incident reports by phone through a toll free telephone number (or numbers), by email, or from other workstations. This client will interface with all Help Desk operational processes such as call handling (receipt and routing), call or problem logging, tracking, problem resolution, and status reporting. Some other key features of the Help Desk client include:

- Web interface
- Intelligent ticket management
- Powerful searching capabilities (easily track clients, tickets, assets and FAQs)
- A searchable FAQ knowledge base
- Reporting

Personal Productivity Tools – These are the tools such as Wireless/Personal Digital Assistant (PDA) that use transmission via the airwaves and serves as an organizer for personal information. It generally includes at least a name-and-address database, to-do list, and note taker.

Pervasive Device Interfaces – Pervasive computing enables enterprises, telephone service providers, Internet Service Providers (ISPs), and Application Service Providers (ASPs) to leverage all of their data assets regardless of disparate protocols, language, and formats. E-business content can now be delivered effectively, efficiently, and economically to anywhere, and to any device.

Pervasive device configurations range from embedded machine devices without a user interface to devices with multi-modal interfaces such as traditional keyboard and mouse interfaces, small text screens, pen, touch screens, speech-to-text, text-to-speech, and other emerging technologies.

Desktop Interface – Defines the interface that provides a highly consolidated view of data residing on multiple pages of the underlying application systems. This interface highlights actions and assists navigation throughout the user-interaction. Some key requirements for a unified desktop interface include seamless integration of all of agent applications into one powerful solution, task reduction through process automation, and single sign-on for multiple applications and systems.

Terminal Emulator – A terminal emulator is a graphical application run within the X Window System that emulates a terminal - a text-based console. In other words, it is the window to the command line while concurrently running a GUI. Terminal emulators vary on their aesthetics, feature sets, and resource usage, but all provide a means of interacting with the shell.

Delivery Channels

Delivery Channels define the level of access to applications and systems based upon the type of network used to deliver them.

Internet - The Internet is a worldwide system of computer networks in which users at any one computer can, if they have permission, get information from any other computer.

Intranet - An intranet is a private network that is contained within an enterprise. It may consist of many inter-linked local area networks and is used to share company information and resources among employees.

Extranet - An extranet is a private network that uses the Internet protocol and the public telecommunication system to securely share part of a business's information or operations with suppliers, vendors, partners, customers, or other businesses. An extranet can be viewed as part of a company's intranet that is extended to users outside the company.

Peer to Peer (P2P) - Peer to peer represents a class of applications, operating outside the DNS system and has significant or total autonomy from central servers that take advantage of resources available on the Internet.

Virtual Private Network (VPN) – VPN is a private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures.

Service Requirements

Service Requirements define the necessary aspects of an application, system or service to include legislative, performance, and hosting.

Legislative / Compliance - Defines the pre-requisites that an application, system, or service must have mandated by Congress or governing bodies.

Section 508 – Section 508 requires that Federal agencies' electronic and information technology is accessible to people with disabilities, including employees and members of the public.

Web Content Accessibility - Refers to hardware and software that helps people who are physically or visually impaired.

Security - Policy and procedures that protect data against unauthorized access, use, disclosure, disruption, modification, or destruction.

Privacy: Platform for Privacy Preferences (P3P) – A specification that will allow users' Web browsers to automatically understand Web sites' privacy practices. Privacy policies will be embedded in the code of a Web site. Browsers will read the policy then automatically provide certain information to specific sites based on the preferences set by the users. P3P is based on W3C specifications that have already been established, including HTTP, XML and Resource

Description Framework (RDF). *Privacy* is policy that deals with the degree to which an individual can determine which personal information is to be shared with whom and for what purpose.

Privacy: Liberty Alliance – The Liberty Alliance Project is an alliance formed to deliver and support a federated network identity solution for the Internet that enables single sign-on for consumers as well as business users in an open, federated way. A federated network identity model will enable every business or user to manage their own data, and ensure that the use of critical personal information is managed and distributed by the appropriate parties, rather than a central authority. *Privacy* is policy that deals with the degree to which an individual can determine which personal information is to be shared with whom and for what purpose.

Authentication / Single Sign-on (SSO) – Refers to a method that provides users with the ability to log-in one time and get authenticated access to all their applications and resources.

Hosting – Refers to the service provider who manages and provides availability to a website or application, often bound to a Service Level Agreement (SLA). The Hosting entity generally maintains a server farm with network support, power backup, fault tolerance, load-balancing, and storage backup.

Internal Hosting (within Agency) – Internal hosting refers to the hosting of a website or application within an Agency. The Agency is responsible for the maintenance, support and availability of the website or application.

External Hosting (ISP/ASP/FirstGov) – External hosting means the outsourcing of a website or application with a managed service provider. An Internet Service Provider (ISP) provides telecommunications circuits, server co-location, and website and application hosting. An Application Service Provider (ASP) offers software-based services for high-end business applications and specific-needs applications such as payroll, sales force automation, and human resources. FirstGov is the official managed service provider for the Federal Government.

Service Transport

Service Transport defines the end-to-end management of the communications session to include the access and delivery protocols.

Supporting Network Services - These consist of the protocols that define the format and structure of data and information that is either accessed from a directory or exchanged through communications.

Internet Message Access Protocol / Post Office Protocol (IMAP / POP3) – IMAP allows a client to access and manipulate electronic mail messages on a server. IMAP permits manipulation of remote message folders, called "mailboxes," in a way functionally equivalent to local mailboxes. IMAP also provides the capability for an offline client to resynchronize with the server. POP3 is the most commonly used protocol for retrieving e-mail from a mail host.

Multipurpose Internet Mail Extensions (MIME) – MIME extends the format of Internet mail to allow non-US- American Standard Code for Information Interchange (ASCII) textual messages, non-textual messages, multi-part message bodies, and non-US-ASCII information in message headers. MIME support allows compliant email clients and servers to accurately communicate embedded information to internal and external users.

Simple Mail Transfer Protocol (SMTP) – SMTP facilitates transfer of electronic-mail messages. It specifies how two systems are to interact, and the format used to control the transfer of electronic mail.

Extended Simple Mail Transfer Protocol (ESMTP) - ESMTP allows new service extensions to SMTP to be defined and registered with Internet Assigned Numbers Authority (IANA).

T.120 – T.120, an International Telecommunications Union (ITU) standard, contains a series of communication and application protocols and services that provide support for real-time, multipoint data communications. These multipoint facilities are important building blocks for collaborative applications, including desktop data conferencing and multi-user applications.

H.323 – H.323, an International Telecommunications Union (ITU) standard, addresses Video (Audiovisual) communication on Local Area Networks, including Corporate Intranets and packet-switched networks generally.

Simple Network Management Protocol (SNMP) - SNMP eliminates several of the security vulnerabilities in earlier version.

Lightweight Directory Access Protocol (LDAP) - LDAP is a subset of X.500 designed to run directly over the TCP/IP stack. LDAP is, like X.500, an information model and a protocol for querying and manipulating it. LDAPv3 is an update developed in the IETF (Internet Engineering Task Force), which address the limitations found during deployment of the previous version of LDAP.

Directory Services (X.500) – This is a network service that discovers and identifies resources on a network and makes them accessible to users and applications. The resources include users, e-mail addresses, computers, mapped drives, shared folders, and peripherals such as printers and PDA docking stations. Users and computers access these resources without needing to know how or where the resources are connected.

Dynamic Host Configuration Protocol (DHCP) – A protocol for assigning dynamic IP addresses to devices on a network. A device can receive a different IP address for every connection. Dynamic addressing provides reduced network administration over deploying and connecting user and peripheral devices.

Domain Name System (DNS) – A protocol used for translating domain names (i.e. www.feapmo.gov) to their respective IP addresses. DNS is collectively a network of devices which store query results. As one DNS server or device cannot provide the translated IP address, it queries other DNS devices. This process is invisible to the user.

Border Gateway Protocol (BGP) – Refers to a routing protocol used to exchange routing information between routers on a network, enabling more efficient routing of data.

X.400 – An ISO and ITU standard for e-mail message addressing and transporting. X.400 supports Ethernet, X.25, TCP/IP and dial-up transport methods.

Service Transport - These consist of the protocols that define the format and structure of data and information either accessed from a directory or exchanged through communications.

Transport Control Protocol (TCP) - TCP provides transport functions, which ensures the total amount of bytes sent is received correctly at the destination.

Internet Protocol (IP) - This is the protocol of the Internet and has become the global standard for communications. IP accepts packets from TCP, adds its own header and delivers a "datagram" to the data link layer protocol. It may also break the packet into fragments to support the maximum transmission unit (MTU) of the network.

Hyper Text Transfer Protocol (HTTP) - The communications protocol used to connect to servers on the World Wide Web. Its primary function is to establish a connection with a web server and transmit HTML pages to the client browser.

Hyper Text Transfer Protocol Secure (HTTPS) - The protocol for accessing a secure Web server. Using HTTPS in the URL instead of HTTP directs the message to a secure port number rather than the default Web port number of 80. The session is then managed by a security protocol.

Wireless Application Protocol (WAP) - The Wireless Application Protocol (WAP) is an open, global specification that empowers users of digital mobile phones, pagers, personal digital assistants and other wireless devices to securely access and interact with Internet/intranet/extranet content, applications, and services.

File Transfer Protocol (FTP) - A protocol used to transfer files over a TCP/IP network (Internet, UNIX, etc.). For example, after developing the HTML pages for a Web site on a local machine, they are typically uploaded to the Web server using FTP.

IP Security (IPSEC) – A set of protocols used to secure IP packet exchange. Tunnel and Transport are the two (2) modes supported by IPSEC. IPSEC uses certificates and Public Keys to authenticate and validate the sender and receiver.

Internet Protocol Routing (IP) - Routers exchange connectivity information with other routers to determine network connectivity and adapt to changes in the network. This enables routers to determine, on a dynamic basis, where to send IP packets.

Local Area Network Access - While no specific LAN technology is mandated, the following is required for interoperability in a joint environment. This requires provision for a LAN interconnection. Ethernet, the implementation of Carrier Sense Multiple Access with Collision Detection (CSMA/CD), is the most common LAN technology in use with TCP/IP. The hosts use a CSMA/CD scheme to control access to the transmission medium. An extension to Ethernet, Fast Ethernet provides interoperable service at both 10 Mbps and 100 Mbps. Higher-speed interconnections are provided by 100BASE-TX (two pairs of Category 5 unshielded twisted pair, with 100BASE-TX Auto-Negotiation features employed to permit interoperation with 10BASE-T).

Point-to-Point - The point-to-point standards are designed for single links that transport packets between two peers. These links provide full-duplex, simultaneous, bi-directional operation, and are assumed to deliver packets in order.

Hosting - Hosts are computers that generally execute application programs on behalf of users and share information with other hosts. Internet Engineering Task Force (IETF) Standard 3 is an umbrella standard that references other documents and corrects errors in some of the referenced documents. IETF Standard 3 also adds additional discussion and guidance for implementers. IETF Standard 3 consists of Request for Comments (RFC) 1122 and RFC 1123. This pair of documents defines and discusses the requirements for host system implementations of the IP suite. RFC 1122 covers the communications protocol layers (i.e., link layer, IP layer, and transport layer). RFC 1123 covers the application layer protocols.

2.2.2 Service Platform and Infrastructure

The Service Platform and Infrastructure Area, as illustrated in Figure - 5, defines the collection of platforms, hardware and infrastructure specifications that enable Component-Based Architectures and Service Component re-use.

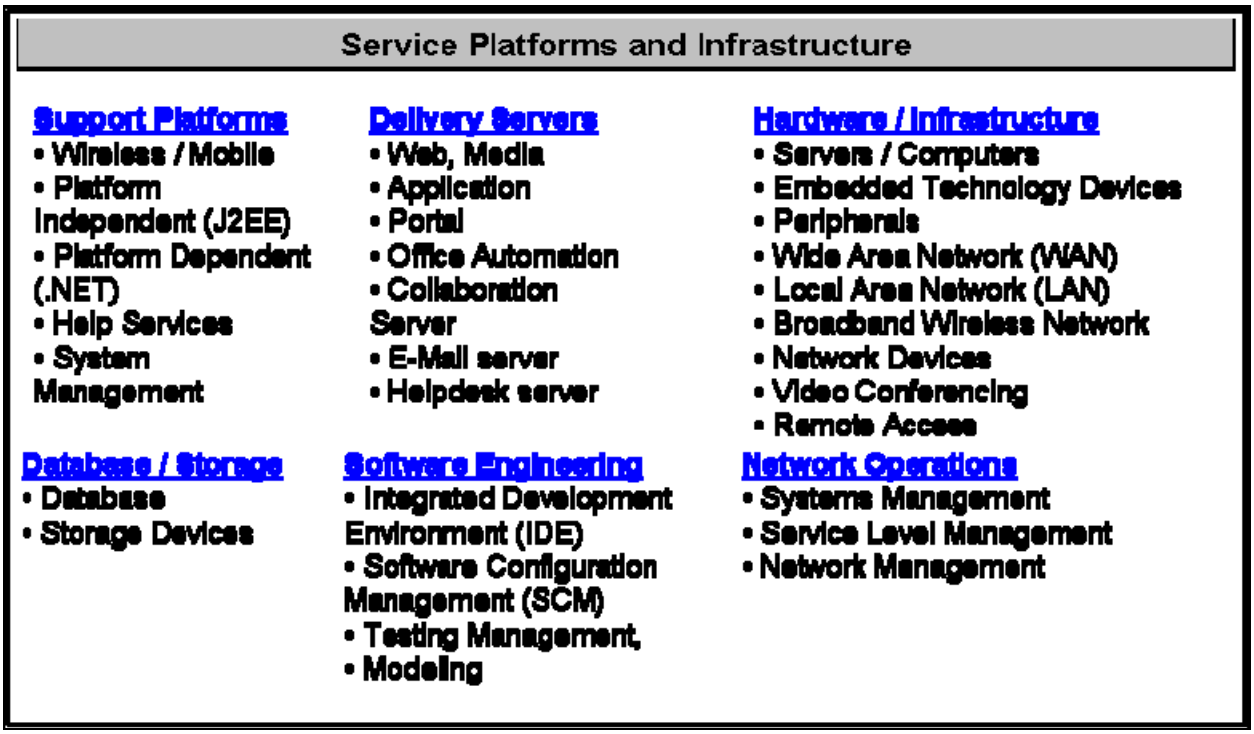


Figure 5 -- Service Categories for "Service Platforms and Infrastructure"

Service Categories, Standards, and Specifications for the service area "Service Platforms and Infrastructure" are defined below:

Supporting Platforms

Supporting platforms are hardware or software architectures. The term originally dealt with only hardware, and it is still used to refer to a CPU model or computer family.

Wireless / Mobile – Communication using radio transmission via the airwaves. Various communications techniques are used to provide wireless transmission including infrared line of sight, cellular, microwave, satellite, packet radio and spread spectrum.

Platform Independent – Defines the operating systems and programming languages that are able to execute and run on any platform or operating system. A platform is the underlying hardware and software comprising a system.

Platform Dependent – Defines the operating systems and programming languages that are able to execute and run on a specific platform or operating system. A platform is the underlying hardware and software comprising a system.

Help Services – Help Services are the virtual extension of an organization's business operations, managing technology questions and problems raised by end users from receipt of the initial call through final problem resolution. Help Services typically provide a single-point-of-contact

(SPOC) for logging, tracking, reporting, and management through resolution of IT problems. Problem Management includes documenting problems, routing those problems to the appropriate personnel for resolution, recognizing recurring problems, reducing the impact of problems, and reducing the number of problems that occur.

System Management – Refers to enterprise-wide administration of distributed computer systems and is strongly influenced by network management initiatives in telecommunications. System management may involve one or more of the following tasks:

- Hardware inventories.
- Server availability monitoring and metrics.
- Software inventory and installation.
- User's activities monitoring.
- Capacity monitoring.
- Security management.
- Storage management.
- Network capacity and utilization monitoring.

Delivery Servers

Delivery Servers are front-end platforms that provide information to a requesting application. It includes the hardware, operating system, server software, and networking protocols.

Web Servers – provide World Wide Web services on the Internet. It includes the hardware, operating system, Web server software, TCP/IP protocols and the Web site content (Web pages). If the Web server is used internally within an Agency or an organization and not by the public, it may be known as an "intranet server."

Media Servers – provide optimized management of media-based files such as audio and video streams and digital images.

Application Servers – performs the business logic, although some part may still be handled by the user's machine. Application servers may be Web–based in an internet environment.

Portal Servers – represent focus points for interaction, providing integration and single-source corporate information.

Office Automation – Office Automation refers to the varied computer hardware and software used to digitally create, collect, store, manipulate, and relay office information needed for accomplishing basic tasks and goals. Raw data storage, electronic transfer, and the management of electronic business information comprise the basic activities of an office automation system. Office automation helps in optimizing or automating existing office procedures.

Collaboration Server – Enables organizations to collaborate by bringing employees, customers, suppliers, and partners into a collaborative digital workplace. The *collaboration server* is a machine accessible by collaboration clients over a network that includes features such as Synchronous / Asynchronous Collaboration, Document Sharing and Co-Authoring, Activity Tracking and Notification, and Enterprise Integration.

E-Mail Server – Mail server is an application that receives email from email clients or other mail servers. It is the workhorse of the email system. A mail server usually consists of a storage area, a set of user definable rules, a list of users and a series of communication modules. The storage area is where mail is stored for local users, and where messages that are in transit to another destination are temporarily stored. It usually takes the form of a simple database of information. Most mail servers are designed to operate without any manual intervention during normal operation. They wait for a message to be sent to them and process it accordingly, or collect messages from other mail servers at predetermined intervals.

Help Desk Server – Help Desk Server is software that creates a help desk website instantly accessible with a web browser. Help Desk Server provides typically provides problem management and tracking, call management, and knowledge repository. It may include advanced features such as Frequently-Asked-Questions (FAQ), discussion forum, asset/inventory management, and request type and location based service request routing.

Database / Storage

Database / Storage refers to a collection of programs that enables storage, modification, and extraction of information from a database, and various techniques and devices for storing large amounts of data.

Database – Refers to a collection of information organized in such a way that a computer program can quickly select desired pieces of data. A database management system (DBMS) is a software application providing management, administration, performance, and analysis tools for databases.

Storage – Storage devices are designed to provide shared storage access across a network. These devices provide extended storage capabilities to the network with reduced costs compared to traditional file servers.

> *Network-Attached Storage* (*NAS*) – A NAS device is a server dedicated to nothing more than file sharing.
>
> *Storage Area Network (SAN)* – A SAN is a high-speed sub-network of shared storage devices. A storage device is a machine that contains nothing but a disk or disks for storing data.

Hardware / Infrastructure

Hardware / Infrastructure define the physical devices, facilities and standards that provide the computing and networking within and between enterprises.

Servers / Computers – This refers to the various types of programmable machines which are capable of responding to sets of instructions and executing programs.

Enterprise Server – A computer or device on a network that manages network resources and shared applications for multiple users.

Mainframe – A very large computer capable of supporting hundreds, or even thousands, of users simultaneously. Mainframes support simultaneous programs.

Embedded Technology Devices – This refers to the various devices and parts that make up a server or computer as well as devices that perform specific functionality outside of a server or computer.

Random Access Memory (RAM) – A type of computer memory that can be accessed randomly; that is, any byte of memory can be accessed without touching the preceding bytes. RAM is the most common type of memory found in computers and other devices, such as printers.

Microprocessor - A silicon chip that contains a CPU. In the world of personal computers, the terms microprocessor and CPU are used interchangeably. At the heart of all personal computers and most workstations sits a microprocessor.

Redundant Array of Independent Disks (RAID) – An assembly of disk drives that employ two or more drives in combination for fault tolerance and performance. RAID disk drives are used frequently on servers but aren't generally necessary for personal computers. RAID is generally configured as mirrored or striped. Mirrored RAID (Level 1) provides a fail-over drive. Striped RAID (Levels 0, 3, and 5) write data across multiple disk drives so a single disk failure can be recovered from the data on the remaining drives. There are three (3) types of RAID systems: failure-resistant disk systems (protects against data loss due to disk failure), failure-tolerant disk systems (protects against loss of data access due to failure of any single component), and disaster-tolerant disk systems (consists of two or more independent zones, either of which provides access to stored data).

Peripherals – Computer devices that are not part of the essential computer (i.e. the memory and microprocessor). Peripheral devices can be external and internal.

Network Devices / Standards - A group of stations (computers, telephones, or other devices) connected by communications facilities for exchanging information. Connection can be permanent, via cable, or temporary, through telephone or other communications links. The transmission medium can be physical (i.e. fiber optic cable) or wireless (i.e. satellite).

Video Conferencing - Communication across long distances with video and audio contact that may also include graphics and data exchange. Digital video transmission systems typically consist of camera, codec (coder-decoder), network access equipment, network, and audio system.

Network Operations

Network Operations involves the capability for monitoring and managing systems and related infrastructure at an enterprise-level, the capability for managing user and asset identity and authentication at an enterprise-level, the capability for managing the configuration of systems and software at an enterprise-level, and the capability to assure that new and transitioned systems maintain an appropriate level of confidentiality, integrity, authentication, non-repudiation, and availability.

System Management - Systems Management provides the capability to manage designated systems and information services. This includes: the capability to review and publish addresses of system objects; monitor the status of objects; start, restart, reconfigure, or terminate network or system services; and detect loss of system objects in order to support automated fault recovery.

Service Level Management – Service Level Management provides the ability of a network to ensure predetermined traffic and service requirements of network and service elements (e.g., end-system, router, or an application) can be satisfied.

Network Management - Network Management provides the capability to manage designated networks. This includes: controlling the network's topology; dynamically segmenting the network into multiple logical domains; maintaining network routing tables; monitoring the network load; and making routing adjustments to optimize throughput.

Software Engineering

Software engineering refers to the support environment for development, modeling, testing, and versioning. The Technical Model is concerned with component technical architecture, not engineering processes.

Integrated Development Environment (IDE) – This consists of the hardware, software and technology that facilitate the development of software applications and systems. An IDE normally consists of a source code editor, a compiler and/or interpreter, build automation tools, and (usually) a debugger. Sometimes a version control system and various tools are integrated to simplify the construction of a GUI. Many modern IDEs also have a class browser, an object inspector, and a class hierarchy diagram, for use with object oriented software development.

IDEs are designed to maximize programmer productivity by providing tightly-knit components with similar user interfaces, thus minimizing the amount of mode switching the programmer must do comparing to loose, discrete collections of disparate development programs.

Software Configuration Management – Technology applicable to all aspects of software development from design to delivery specifically focused on the control of all work products and artifacts generated during the development process. Several technical solutions on the market provide the integration of the software configuration management functions.

Test Management – Technology which supports the consolidation of all testing activities and results. Test Management activities include test planning, designing (test cases), execution, reporting, code coverage, and heuristic and harness development.

Modeling – Technology support the process of representing entities, data, business logic, and capabilities for aiding in software engineering.

2.2.3 Component Framework

The Component Framework Area, as illustrated in Figure - 6 , defines the underlying foundation and technical elements by which Service Components are built, integrated and deployed across Component-Based and Distributed Architectures. The Component Framework consists of the design of application or system software that incorporates interfaces for interacting with other programs and for future flexibility and expandability. This includes, but is not limited to, modules that are designed to interoperate with each other at runtime. Components can be large or small, developed in different development environments, and may be platform independent. Components can be executed on stand-alone machines, a LAN, Intranet or on the Internet.

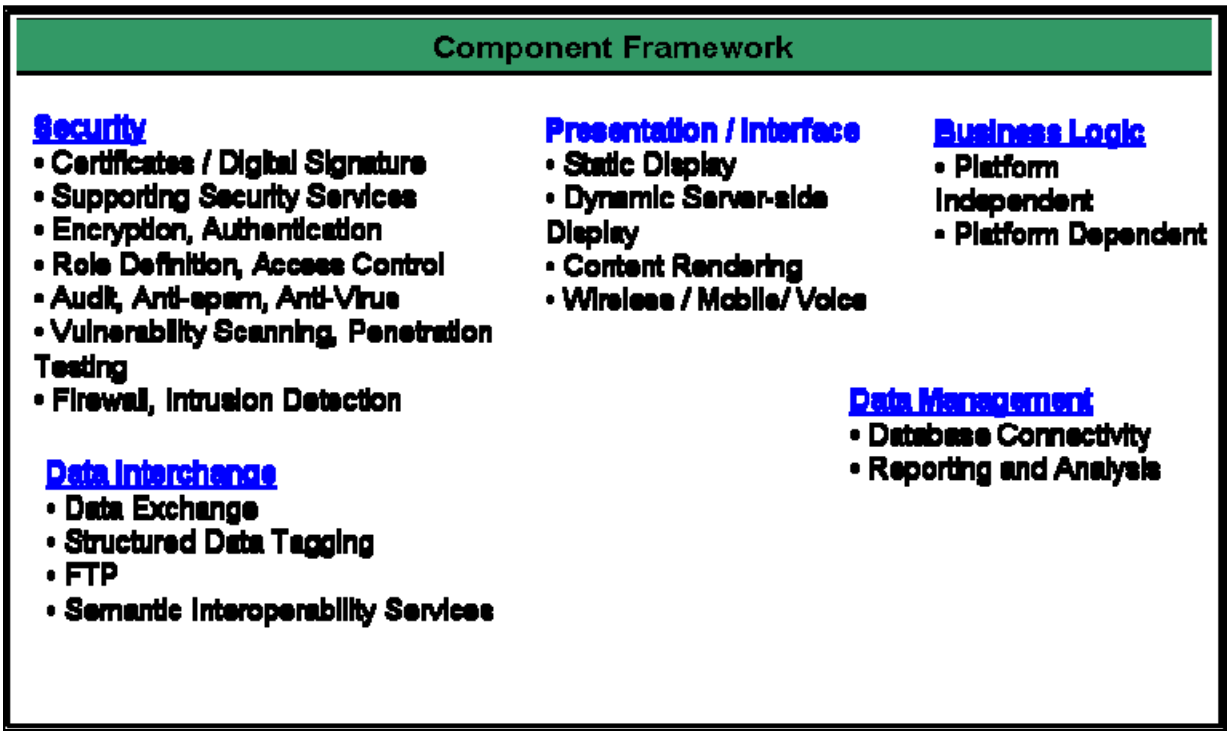


Figure 6 -- Service Categories for "Component Framework"

Service Categories, Standards, and Specifications for the service area “Component Framework” are defined below:

Security

Security defines the methods of protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality and availability. Biometrics, two-factor identification, encryption, and technologies based on the NIST FIPS-140 standards are evolving areas of focus.

Certificates / Digital Signature - Software used by a certification authority (CA) to issue digital certificates and secure access to information. The evolution of Public Key Infrastructure (PKI) is based on the verification and authentication of the parties involved in information exchange.

> *Digital Certificate Authentication* – Authentication implementation for controlling access to network and internet resources through managing user identification. An electronic document – a digital certificate – is issued and used to prove identity and public key ownership over the network or internet.
>
> *Secure Sockets Layer (SSL)* – an open, non-proprietary protocol for securing data communications across computer networks. SSL is sandwiched between the application protocol (such as HTTP, Telnet, FTP, and NNTP) and the connection protocol (such as TCP/IP, UDP). SSL provides server authentication, message integrity, data encryption, and optional client authentication for TCP/IP connections.

Supporting Security Services - These consist of the different protocols and components to be used in addition to certificates and digital signatures.

> *Secure Multipurpose Internet Mail Extensions (S/MIME)* – provides a consistent way to send and receive secure MIME data. Based on the Internet MIME standard, S/MIME provides cryptographic security services for electronic messaging applications: authentication, message integrity and non-repudiation of origin (using digital signatures) and data confidentiality (using encryption). S/MIME is not restricted to mail; it can be used with any transport mechanism that transports MIME data, such as HTTP.
>
> *Transport Layer Security (TLS)* – provides communications privacy over the Internet. The protocol allows client/server applications to communicate in a way designed to prevent eavesdropping, tampering, or message forgery.
>
> *Web Services Security (WS-Security)* – describes enhancements to SOAP messaging to provide message integrity, message confidentiality, and single message authentication. These mechanisms can be used to accommodate a wide variety of security models and encryption technologies including X.509, Kerberos, and SAML.
>
> *Security Assertion Markup Language (SAML)* – an XML-based framework for exchanging security information expressed in the form of assertions about subjects, where a subject is an entity (either human or computer) that has an identity in some security domain. SAML is expected to play a key role in the Federal-wide e-authentication initiative, and is supported by the Liberty Alliance and WS-Security.

Simple Key Management Protocol (SKIP) – a protocol developed by Sun Microsystems to handle key management across IP networks and VPNs.

Secure Shell (SSH) – a method of performing client authentication. Because it supports authentication, compression, confidentiality and integrity, SSH is used frequently on the Internet. SSH has two important components, RSA certificate exchange for authentication and Triple DES for session encryption.

Cryptography – method used to support the Public Key Infrastructure, which is a system of Certificate Authorities that perform some set of certificate management, archive management, key management, and token management functions for a community of users.

Environment Management – services to integrate and manage the execution of platform services for particular applications and users. These services are invoked via an easy-to-use, high-level interface that enables users and applications to invoke platform services without having to know the details of the technical environment. The environment management service determines which platform service is used to satisfy the request and manages access to it through the API.

Security Layers (Physical, Link, Network) - The physical layer, Layer 1 of the OSI 7 Layer Reference Model, provides the mechanical, electrical, functional, and procedural means to activate, maintain, and deactivate physical connections for bit transmission between data-link entities. The (data) link layer is layer 2 of the Open Systems Interconnect (OSI) 7 Layer Reference Model where a point-to-point communication channel connecting two sub–network relays is established. The Network layer is layer 3 of the Open Systems Interconnect (OSI) 7 Layer Reference Model.

Encryption – Encryption refers to algorithmic schemes that encode plain text into non-readable form, providing privacy. The receiver of the encrypted text uses a "key" to decrypt the message, returning it to its original plain text form. The key is the trigger mechanism to the algorithm. There are many types of encryption and not all of it is reliable. The same computer power that yields strong encryption can be used to break weak encryption schemes. Initially, 64-bit encryption was thought to be quite strong, but today 128-bit encryption is the standard. Strong encryption makes data private, but not necessarily secure. To be secure, the recipient of the data, often a server, must be positively identified as being the approved party. This is usually accomplished online using digital signatures or certificates.

Authentication – Authentication is the process to verify that someone is who they claim they are. This usually involves a username and a password, but can include any other method of demonstrating identity, such as a smart card, retina scan, voice recognition, or fingerprints. There are three main algorithms for authentication: passwords, Needham and Schroeder protocol (used in Kerberos), and public key encryption. In all of them, the central issue is to never allow the

secret information outside a secured environment, while at the same time allowing the recipient to verify that the secret was used.

Role Definition, Access Control – Role-based security is by far the most elegant and productive way to provide user authorization and access checks for your application. A role is a category of users who share the same security privileges. Role-based security allows administrators to assign access permissions to users based on the roles they play rather than on their individual identities. These privileges can be used to control access to objects and methods, and are easier to identify and maintain than user-based security. Roles can have overlapping responsibilities and privileges; that is, users belonging to different roles may need to perform common operations. Access control is a much more general way of talking about controlling access to a web resource. Access can be granted or denied based on a wide variety of criteria, such as the network address of the client, or the roles. Restricting access based on something other than the identity of the user is generally referred to as *Access Control*. With role-based access control, access decisions are based on the roles that individual users have as part of an organization. Access rights are grouped by role name, and the use of resources is restricted to individuals authorized to assume the associated role.

Audit, Anti-spam, Anti-virus – The audit measures the organization's security policy and provides an analysis of the effectiveness of that policy within the context of the organization's structure, objectives and activities. Audit is concerned primarily with how security policies are actually used. Following are some of the key questions that security audit evaluate:

- Are passwords difficult to crack?
- Are there access control lists (ACLs) in place on network devices to control who has access to shared data?
- Are there audit logs that show who accessed data?
- Are the audit logs reviewed?
- Are the security settings for operating systems in accordance with accepted industry security practices?
- Have all unnecessary applications and computer services been eliminated for each system?
- Are these operating systems and commercial applications patched to current levels?
- Is there a disaster recovery plan? Have the participants and stakeholders ever rehearsed the disaster recovery plan?
- Are there adequate cryptographic tools in place to govern data encryption, and have these tools been properly configured?
- Have custom-built applications been written with security in mind?
- How have these custom applications been tested for security flaws?
- How are configuration and code changes documented at every level? How are these records reviewed and who conducts the review?

Vulnerability Scanning – Vulnerability scanning typically refers to the scanning of systems connected to the Internet but can also refer to system audits on internal networks not connected to the Internet in order to assess the threat of rogue software or malicious employees in an enterprise. Vulnerability scanning employs software that seeks out security flaws based on a

database of known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the network's security.

Penetration Testing – Penetration testing is a method of evaluating the security of a computer system or network by simulating an attack by a malicious user, known as a cracker (though often incorrectly referred to as a hacker). The process involves an active analysis of the system for any potential vulnerabilities that may result from poor or improper system configuration, known and/or unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures. Near flawless penetration testing is a requirement for high-rated secure systems, those rated above B1 based on the Trusted Computer System Evaluation Criteria (TCSEC) and its Trusted Network and Database Interpretations (TNI and TDI). Unlike security functional testing, which demonstrates correct behavior of the product's advertised security controls, penetration testing is a form of stress testing which exposes weaknesses — that is, flaws — in the *trusted computing base* (TCB).

Firewall – A firewall is a dedicated appliance, or software running on another computer, which inspects network traffic passing through it, and denies or permits passage based on a set of rules. Basically, a firewall, working closely with a router program, examines each network packet to determine whether to forward it toward its destination. A firewall also includes or works with a proxy server that makes network requests on behalf of workstation users. A firewall is often installed in a specially designated computer separate from the rest of the network so that no incoming request can get directly at private network resources. Generally, firewalls are configured to protect against unauthenticated interactive logins from the "outside" world. Firewalls can't protect against attacks that don't go through the firewall or against tunneling over most application protocols to trojaned or poorly written clients.

Intrusion Detection – Defines an intrusion is an attempt to break into or misuse a computer system or network. An intrusion detection system, attempts to detect an intruder breaking into your system or a legitimate user misusing system resources. The intrusion detection system should run constantly on your system, working away in the background, and only notifying you when it detects something it considers suspicious or illegal. What is suspicious or illegal depends on the security policy you have established for the system.

Presentation / Interface

This defines the connection between the user and the software, consisting of the presentation that is physically represented on the screen.

Static Display - Static Display consists of the software protocols used to create a pre-defined, unchanging graphical interface between the user and the software.

> *Hyper Text Markup Language (HTML)* - The language used to create Web documents and a subset of Standard Generalized Markup Language (SGML).
>
> *Standard Generalized Markup Language (SGML)* - A standard methodology with formal syntax for adding information to a document relating to its structure and/or content by

applying identifiers for elements of information in a neutral way, stored in a neutral form, independent of systems, devices, and applications. HTML and XML are examples of SGML-based document markup languages.

Dynamic / Server-Side Display - This consists of the software used to create graphical user interfaces with the ability to change while the program is running.

Content Rendering - This defines the software and protocols used for transforming data for presentation in a graphical user interface.

Wireless / Mobile / Voice - Consists of the software and protocols used for wireless and voice-enabled presentation devices.

Business Logic

Defines the software, protocol or method in which business rules are enforced within applications.

Platform Independent - Consists of all software languages that are able to execute and run on any type of operating system or platform.

Enterprise Java Beans (EJB) – EJB Server is a component transaction server. It supports the EJB server-side component model for developing and deploying distributed, enterprise-level applications in a multi-tiered environment. It provides the framework for creating, deploying, and managing middle-tier business logic. EJB components (or Beans) are reusable modules of code that combine related tasks (methods) into a well-defined interface. EJB components contain the methods that execute business logic and access data sources.

Platform Dependent - Consists of the programming languages and methods for developing software on a specific operating system or platform.

Data Interchange

Define the methods in which data is transferred and represented in and between software applications.

Data Exchange – Data Exchange is concerned with the sending of data over a communications network and the definition of data communicated from one application to another. Data Exchange provides the communications common denominator between disparate systems.

XMI - Enables easy interchange of metadata between modeling tools (based on the OMG UML) and metadata repositories (OMG MOF based) in distributed heterogeneous environments. XMI integrates three key industry standards: XML, UML, and MOF. The integration of these three standards into XMI marries the best of OMG and W3C

metadata and modeling technologies, allowing developers of distributed systems to share object models and other metadata over the Internet.

XQuery – A language used for processing and evaluating XML data. The XQuery language provides results of expressions allowing the use of evaluations to the implementation of XQuery.

XML Path Language - XPath is a specialized language for addressing parts of an XML document, designed to be used by XSLT.

XML Digital Signature – XML Digital Signature is a specialized language for applying an XML-encoded digital signature within an XML document, rather than as separate data.

Document Object Model – A programmatic means for read/write random access to XML documents, there are different approaches for accessing XML data, e.g., the Simple API for XML (SAX) approach is used for sequential access and the Java Document Object Model (JDOM) approach is used for a Java-specific binding of Document Object Model (DOM).

XML Forms - XForms architecture separates purpose (semantics) from presentation (syntax), and associates the capabilities of XML and the ease of HTML for a wide range of devices.

Simple Object Access Protocol (SOAP) – SOAP provides HTTP/XML–based remote procedure call capabilities for XML Web Services.

Electronic Business using XML (ebXML) - A modular suite of specifications that enables enterprises to conduct business over the internet: exchanging business messages, conducting trading relationships, communicating data in common terms and defining and registering business processes.

Resource Description Framework (RDF) - RDF provides a lightweight ontology system to support the exchange of knowledge on the Web. It integrates a variety of web-based metadata activities including sitemaps, content ratings, stream channel definitions, search engine data collection (web crawling), digital library collections, and distributed authoring, using XML as interchange syntax.

Web Services User Interface (WSUI) - WSUI uses a simple scheme for describing a WSUI "component" that can be used in a portal to call backend SOAP and XML services. WSUI uses XSLT stylesheets to construct user-facing views to enable users to interact with the services.

Electronic Data Interchange (EDI) – EDI is a concept that has been in commercial use for more than 30 years. It is widely accepted by companies all over the world as the way to electronically exchange business data. An EDI-based information exchange is usually a two-way process. Thus, the translator component will also be used to translate incoming EDI messages into an

application-specific format. An EDI transmission can basically be divided into two logical parts: the message itself and the communication.

Since the goal of EDI is to have a standardized message, a number of different standards have been developed and established over the years. The most commonly used message standards are:

- ANSI ASC X12 - US standard
- EDIFACT - standard recommended by the United Nations, used mainly in Europe
- Others such as HIPAA, VICS, VDA, UCS, etc.

Transportation of the EDI file over a network can be done in many ways. Any network and any protocol can be used as long as it fits the needs. Examples of communication medium are: private Value-Added Networks (VAN) or the Internet (AS1, AS2, FTP, etc.).

Structured Data Tagging – In concept, data tagging uses standard definitions to translate text-based information into machine-readable data files that can be searched, retrieved, and analyzed using computer software tools. Tags, along with their standard definitions, are contained in a vocabulary listing called a Taxonomy. "eXtensible Business Reporting Language" (XBRL) is a specific data tagging language that facilitates a format for enhancing financing and business reporting.

FTP – FTP or File Transfer Protocol is used to transfer data from one computer to another over the Internet, or through a network. Specifically, FTP is a commonly used protocol for exchanging files over any TCP/IP based network to manipulate files on another computer on that network regardless of which operating systems are involved (if the computers permit FTP access). There are many existing FTP client and server programs. FTP servers can be set up anywhere between game servers, voice servers, internet hosts, and other physical servers.

Semantic Interoperability Services – Semantic Interoperability requires that the data types and operations in a service interface can be aligned to a common understanding. Semantic interoperability services which exploit ontology descriptions for realizing a semantic collaboration model for networked organization contexts. There are three types of ontology-based interoperability services, namely, the matching service for performing semantic affinity evaluations on ontology elements, the discovery service for query composition, propagation, and processing, and the acquisition service for information resource access.

Data Management

The management of all data/information in an organization includes data administration, the standards for defining data and the way in which people perceive and use it.

Database Connectivity - Defines the protocol or method in which an application connects to a data-store or database.

Open Database Connectivity (ODBC) – provides a standard software API method for using database management systems (DBMS). The ODBC specification offers a procedural API for using SQL queries to access data. An implementation of ODBC will

contain one or more applications, a core ODBC library, and one or more "database drivers".

Java Database Connectivity (JDBC) – is an industry standard for database-independent connectivity between the Java programming language and a wide range of databases. The JDBC API provides a call-level API for SQL-based database access. JDBC technology allows you to use the Java programming language to exploit "Write Once, Run Anywhere" capabilities for applications that require access to enterprise data.

Reporting and Analysis - Consists of the tools, languages and protocols used to extract data from a data–store and process it into useful information. XML for Analysis (XMLA) is a SOAP-based interface for exposing OLAP and Data Mining data sources as Web services. It advances some of the successful concepts of OLE DB for OLAP to a cross-platform Web service API.

2.2.4 Service Interface and Integration

The Service Interface and Integration Area, as illustrated in Figure - 7 , defines the discovery, interaction and communication technologies joining disparate systems and information providers. Component-based architectures leverage and incorporate Service Interface and Integration specifications to provide interoperability and scalability.

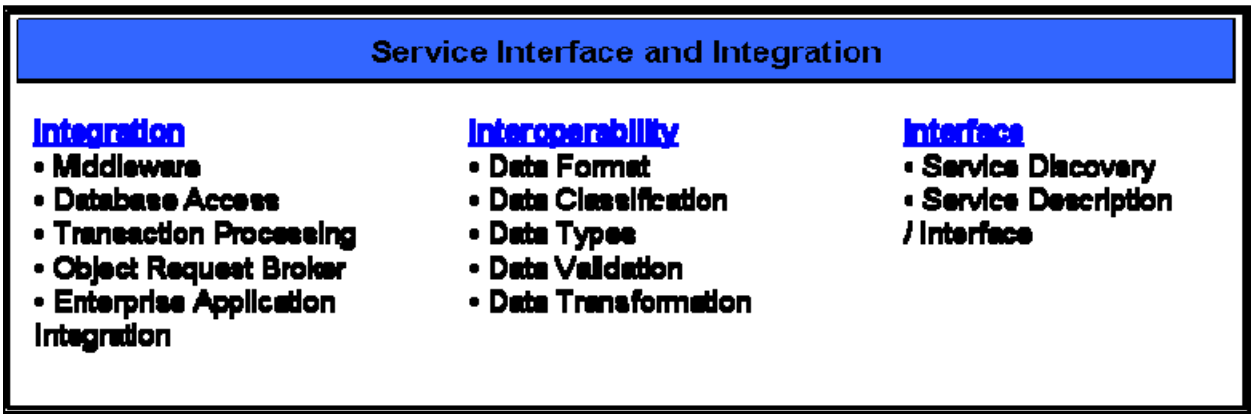


Figure 7 -- Service Categories for "Service Interface and Integration"

Service Categories, Standards, and Specifications for the service area “Service Interface and Integration” are defined below:

Integration

Integration defines the software services enabling elements of distributed business applications to interoperate. These elements can share function, content, and communications across heterogeneous computing environments. In particular, service integration offers a set of architecture services such as platform and service location transparency, transaction management, basic messaging between two points, and guaranteed message delivery.

Middleware – Middleware increases the flexibility, interoperability, and portability of existing infrastructure by linking or "gluing" two otherwise separate applications.

Message oriented Middleware (MOM) – provides capability for integrating and connecting systems across heterogeneous environments which operates on the principles of message queuing and/or message passing. Middleware enables users and developers to interconnect program logic and data between systems or processes using consistently defined interfaces. *Message-Oriented Middleware Integration* is an excellent choice when systems are not reliably connected because there is the potential for network failure or distributed systems failure. Message-oriented middleware capabilities include:

- Asynchronous messaging for process-to-process and application interoperability
- Distributed transaction processing
- Reliable transfer of information between dissimilar networks and applications running on those network
- Guaranteed delivery of messages
- Uniform and orderly message delivery
- Secure messaging, including access control, payload encryption and privacy
- Automated business functions

Transaction Processing Monitor – Software providing synchronous messaging and queuing along with other transaction management services designed to support the efficient processing of high volumes of transactions. Core services include load balancing, rollback/commit, and recovery. Transaction Processing provides cost-effective scalability to applications and database systems by managing and throttling transactions on behalf of the database system.

Object Request Broker (ORB): Common Object Request Broker Architecture (CORBA) – An architecture that enables objects to communicate with one another regardless of what programming language they were written in or what operating system they're running on. Object Request Broker (ORB) is a technology enabling distributed objects to communicate and exchange data with remote objects. ORB encapsulates the locality and implementation of the objects, allowing users to develop applications that leverage components by accessing the components interface.

Service Oriented Integration – provides capability of connecting systems by enabling them to consume and provide XML-based Web services. The interfaces to these systems are described through Web Services Definition Language (WDSL) contracts. Systems interact with each other by using SOAP messages. SOAP messages are usually conveyed through HTTP by using XML serialization. *Service-Oriented Integration* enables interoperability by using Web Services Integration (WS-I) Basic Profile and XML Schema and SOAP to transport and resolve messages. It also allows use of both synchronous and asynchronous messages.

Enterprise Service Bus (ESB) – is a new term in the middleware most commonly used with Service Oriented Architecture (SOA) implementations. Generally, ESB refers to a universal middleware environment that supports simple, speedy, standards-based integration across

heterogeneous network application environments. ESB is an architectural concept that refers to a growing segment of the integration software market that addresses the intersection of message-oriented middleware (MOM) and Web services. ESB technology provides an abstraction layer that mediates among old and new computing platforms and middleware environments. An ESB environment offers simplification along several areas such as:

- Unified integration paradigm: ESB products wrap, virtualize and integrate the legacy integration paradigms-such as MOMs, object request brokers (ORBs) and remote procedure calls (RPCs)-within the new paradigms of Web services and service-oriented architecture.
- Modular integration layers: ESB products allow implementation of as few or as many robust integration services-such as reliable messaging, event notification, publish-and-subscribe, content transformation and orchestration-as appropriate to a particular integration scenario.
- Flexible integration patterns: ESB products support flexible messaging patterns, including hub-and-spoke, routed and peer-to-peer message flows, within the same integration environment. They support the request/response conversational flows associated with SOA, the publish/subscribe flows associated with event-driven architecture, and the method-invocation flows associated with object-invocation environments. And they allow integration architects to implement communication alternatives such as static vs. dynamic object binding; synchronous vs. asynchronous connections; stateless vs. stateful conversations; transacted vs. non-transacted sessions, and reliable vs. best-effort messaging.

Enterprise Application Integration – Refers to the processes and tools specializing in updating and consolidating applications and data within an enterprise. EAI focuses on leveraging existing legacy applications and data sources so that enterprises can add and migrate to current technologies.

Interoperability

Interoperability defines the capabilities of discovering and sharing data and services across disparate systems and vendors.

Data Format / Classification – Defines the structure of a file. There are hundreds of formats, and every application has many different variations (database, word processing, graphics, executable program, etc.). Each format defines its own layout of the data. The file format for text is the simplest.

eXtensible Markup Language (XML) – XML has emerged as the standard format for web data, and is beginning to be used as a common data format at all levels of the architecture. Many specialized vocabularies of XML are being developed to support specific Government and Industry functions.

XML Linking Language (XLINK) – A language used to modify XML documents to include links, similar to hyperlinks, between resources. XLINK provides richer XML content through advanced linking integration with information resources.

Namespaces – Namespaces are qualified references to URI (Uniform Resource Identifier) resources within XML documents.

Electronic Data Interchange (EDI) - Defines the structure for transferring data between enterprises. EDI is used mainly used for purchase-related information. ANSI X.12 refers to the approved EDI standards.

Data Types / Validation – Refers to specifications used in identifying and affirming common structures and processing rules. This technique is referenced and abstracted from the content document or source data.

Document Type Definition (DTD) – DTD is used to restrict and maintain the conformance of an XML, HTML, or SGML document. The DTD provides definitions for all tags and attributes within the document and the rules for their usage. Alterations to the document are validated with the referenced DTD.

XML Schema – XML Schemas define the structure, content, rules and vocabulary of an XML document. XML Schemas are useful in automation through embedding processing rules.

Data Transformation - Data Transformation consists of the protocols and languages that change the presentation of data within a graphical user interface or application.

eXtensible Stylesheet Language Transform (XSLT) - Transforms XML document from one schema into another. Used for data transformation between systems using different XML schema, or mapping XML to different output devices.

Interface

Interface defines the capabilities of communicating, transporting and exchanging information through a common dialog or method. Delivery Channels provide the information to reach the intended destination, whereas Interfaces allow the interaction to occur based on a predetermined framework.

Service Discovery - Defines the method in which applications, systems or web services are registered and discovered.

Universal Description Discovery and Integration (UDDI) - UDDI provides a searchable registry of XML Web Services and their associated URLs and WSDL pages.

Intelligent Agent – An autonomous software component that uses intelligence to do an assigned task; for example, searching through incoming mail and highlighting items related to a certain subject.

Service Description / Interface - Defines the method for publishing the way in which web services or applications can be used.

Web Services Description Language (WSDL) - WSDL is an XML based Interface Description Language for describing XML Web Services and how to use them.

Application Program Interface (API) / Protocol - A language and message format used by an application program to communicate with the operating system or some other control

program such as a database management system (DBMS) or communications protocol. APIs are implemented by writing function calls in the program, which provide the linkage to the required subroutine for execution. Thus, an API implies some program module is available in the computer to perform the operation or it must be linked into the existing program to perform the tasks.

2.2.5 LOB Specific Technical Services

Figure – 8 shows the initial set of HR LOB-specific technical services based upon the target requirements for the HR ”Core” functions, i.e., Personnel-Action procssing, Compensation, and Benefits processing.

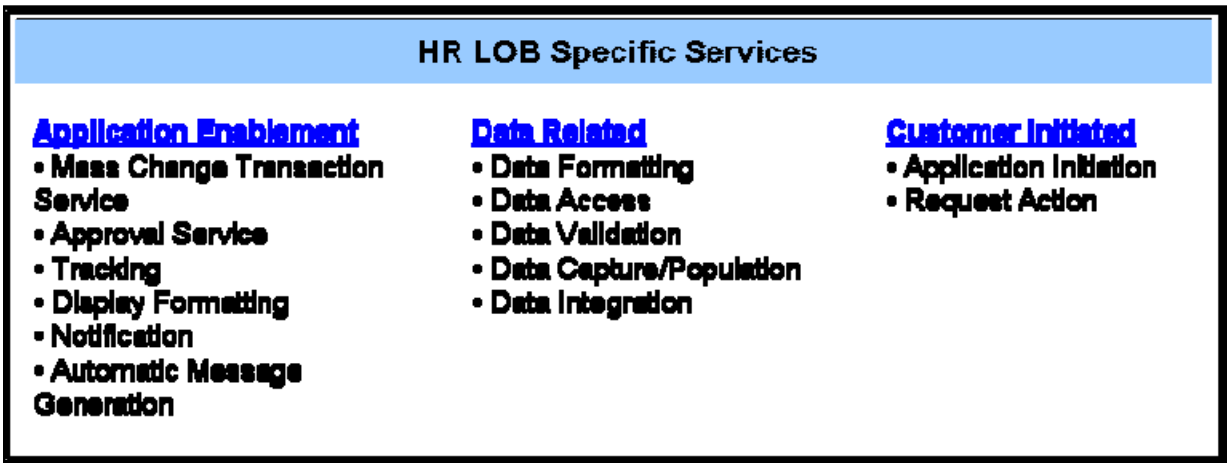


Figure 8 -- HR LOB specific Technical Services

Initiation / Request Action Service
Initiation Service is a technical service that detects transactional (customer data is accessed, updated, or added) or non-transactional events (e.g., date driven events). This technical service is required for web based and non-web based solution to identify the user action, trigger the data validation based upon business rules, trigger the request appropriate transaction, and notification service based upon time-based event. This technical service also detects user inputs and creates a request message for a personnel action, report, or any other transaction.

Mass Change Transaction Services
Mass Change Transaction Services allows power user to configure and execute mass updates. The user is able to choose to have the process update existing rows or add new rows. Both effective dating and effective sequencing are supported. Additional steps are added for previewing and manually editing changes online prior to committing the update to the database. A rollback feature also is included so errors can be reversed if necessary. All of these features provide significantly improved ease of use while safeguarding against errors. The user is able to configure mass update definitions, including the population to process, and then create

transactions, preview transactions, process transactions, and manage transaction statuses. It invokes the transaction processor for real-time access or the batch manager. This service consists of the component for setting up and managing system data available for mass updates and an application class that provides access to transaction processing functionality.

Tracking Services
This technical service provides context sensitive transaction tracking similar to the tracking number used by shipping companies. The service should also track workflow requests, personnel action transactions, and approval status.

Approval Services
This technical service works in conjunction with the workflow services, defines approval authority and approval lists, and level of approvals. It should determine whether a requestor approves their own transaction, if they have sufficient signing authority. It should recognize and flag if the employee is at the top of the hierarchy. It should identify and assign an indicator to the ID of person requesting the transaction for tracking purpose.

Notification Services
This technical service creates a notification message when it receives information from entities in the information producer that monitor and detect a situation, such as information changes or updates that are of interest to service consumers. The notify message sent by the publisher is routed by the notification broker service to the appropriate notification consumer proxy service. The notification broker matches notification messages to the consumers that are subscribed to these notifications.

Automatic Message Generation
This technical service detects events and generates messages in an asynchronous way to notify the event occurrence that is grammatically complete, comprehensible and relevant.

Data Access
A data access service is a service that handles the technical details for a particular kind of data source. Data access services are noun-oriented. These services expose data rather than a set of operations. They are not meant to either extend or reuse some existing application logic. What they are really focused on doing is encapsulating some piece of information and exposing it and making it available. It also defines rules of visibility and data entitlements that allow organization to manage privacy for personnel information, governing accessibility of specific employee data attributes.

Data Validation
This technical service enforces data validation rules to all incoming transactions and data submitted from various applications. It also supports conditional external data validation, meaning that data validation rules may be varied by conditions.

Data / Display Formatting
This technical service defines rules for data formatting and transformation based upon the requirements, for example, capture employee name in the specified format. It also specifies the

rules of data format for reports. Formatting rules define transformation of the source structures into destination structures such as standard transformation rules, ranging from simple field moves to arithmetic and string operations, sorting, and more. This technical service also recognizes the formatting rules and formats the output display based upon the user settings, device standards, and organization standards.

Data Capture / Population

This technical service should provide **Vertical Filtering**, i.e., pass only the data elements the target needs, and **Horizontal Filtering**, i.e., pass only the records that conform to the targets rules.

Data Integration

One of the biggest challenges global organizations face today is the fragmentation of data across disparate enterprise systems. This technical service provides capabilities for the following functions:

- **Joins**: combining fields from multiple sources and storing the combined set.
- **Lookups:** combining fields from records with values from reference tables and storing the combined set.
- **Aggregations**: creation of new data sets derived from the combination of multiple sources and/or records
- **Delta Processing**: identifying changed records from a source data set by comparing the values to the prior set from the source.

2.3 TM Structure from Application Perspective

There are different ways to view a technical model. A technical model can be viewed as an architectural template or pattern used to decompose a complex technical environment into a series of "layers," each having a defined purpose, a set of boundaries, defined interrelationships with other layers, and associated principles and characteristics. This view of the technical model provides an integration framework against which architectural artifacts can be aligned to improve their integration and cohesiveness and provides a guide to help differentiate infrastructure functions from application functions to facilitate the allocation of responsibilities to different implementation projects. The following diagram shows the view of the technical model from the application system perspective with different tiers showing the boundaries and relationship of application, systems, and infrastructure partitions and associated technical services.

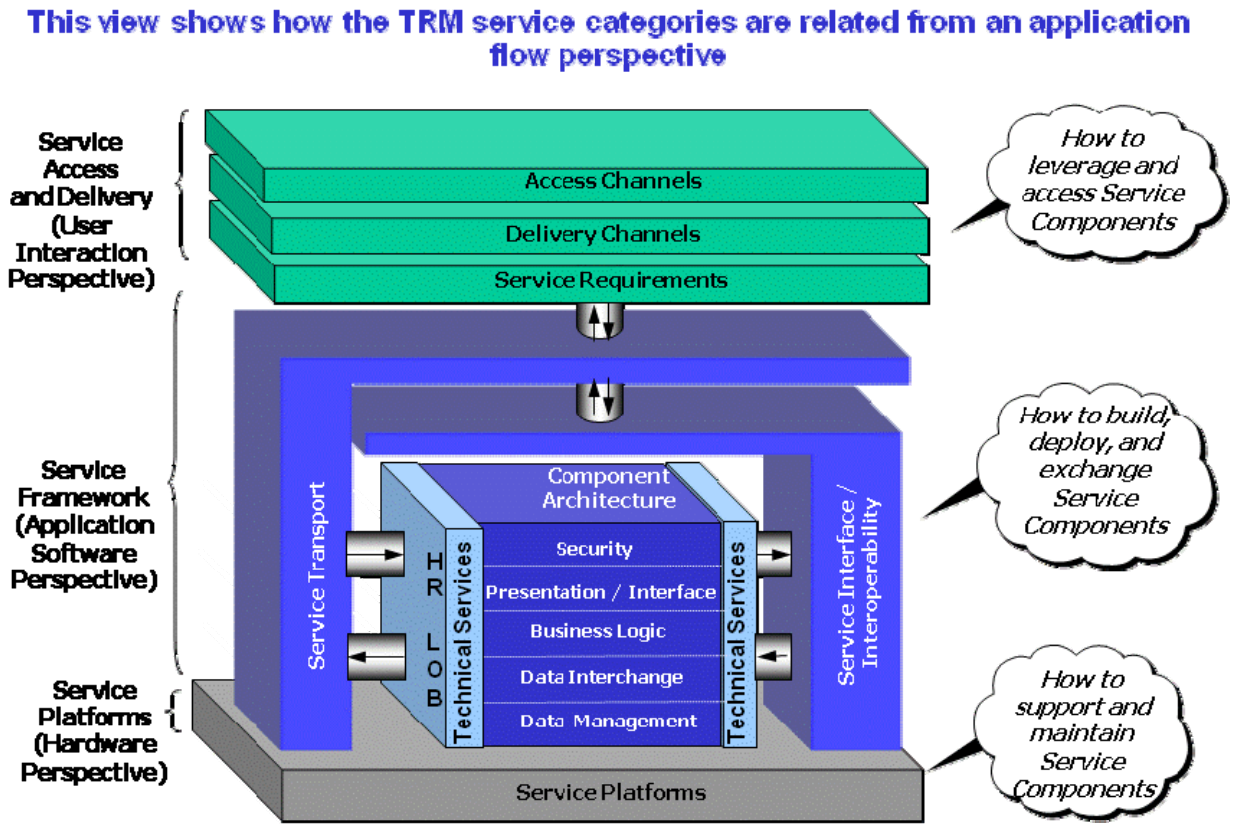


Figure 9 -- HR LOB Technical Model -- Application Flow View

The TM is comprised of three (3) technical tiers to support the construction, exchange, and delivery of component-driven, Service Components. This structure defines: How to leverage and access Service Components, How to build, deploy, and exchange Service Components, and How to support and maintain Service Components.

This view helps in establishing the process-action flow of delivery of service components to the user types by the enabling technology and technical service components. From the structural perspective, an application is composed of multiple logical and / or physical *partitions* that represent presentation logic, business logic, or data management logic. Partitions are hardware independent, have attributes (e.g., language constraints and application frameworks), and use common services and common business objects. This essentially is a view of the threads of execution associated with an application as that application executes end to end.

2.4 Technical Reference Model and Technical Reference Architecture

A reference model is an abstract **framework** for understanding significant relationships among the entities of some environment. It enables the development of specific reference or concrete architectures using consistent standards or specifications supporting that environment. A

reference model consists of a minimal set of unifying concepts, axioms and relationships within a particular problem domain, and is independent of specific standards, technologies, implementations, or other concrete details.

The concepts and relationships defined by the reference model are intended to be the basis for describing references architectures and patterns that will define more specific categories of SOA designs. Concrete architectures arise from a combination of reference architectures, architectural patterns and additional requirements, including those imposed by technology environments.

A *reference architecture* is an architecture that has already been created for a particular area of interest. It typically includes many different architectural styles, applied in different parts of its structure. A *technical reference architecture* is a type of reference architecture that does not directly include structures of application (business) behavior. In other words, it can be used as a base architecture or template for several different application types. It nevertheless still applies only to a specific technical domain.

We use the example of housing to illustrate the difference between the reference model and the reference architecture. The ***reference model*** for the housing includes the framework concepts like roof, foundation, structure, sitting area, eating area, sleeping area, standards for the relative location of the rooms, sizes of the doors and windows, staircases, etc. The role of ***reference architecture*** for housing would be to identify abstract solutions to the problems of providing housing. For example, an abstract solution for housing, one that addresses the needs of its occupants, consists of bedrooms, kitchens, hallways, bathrooms, and so on.

We find that architects and solution providers define the Technical Reference Architecture (TRA) for a solution using the basic constructs that will have specific goals and represent specific architectural style. Again let us consider the building analogy, for example, building architecture style consists of styles such as Cape Cod, Tudor, Contemporary, and Spanish, Ranch. In the realm of HR LOB solutions, the technical reference architecture style or paradigm consists of Service Oriented Architecture (SOA), 3-tier Client/Server, n-tier distributed, etc. HR LOB Solution architects and solution providers will/can define an HR LOB Solution Technical Reference Model using any one of the architecture paradigm based upon the Technical Model.

The reference model defines the applicable standards and the reference architecture selects and applies the standards based upon the architecture style. Therefore, the HR LOB Technical Model serves as a “Building Construction Code” for the HR LOB Solutions. The figure in Appendix – E illustrates this analogy.

Any reference architecture includes both *functional* and *operational* aspects of an IT system. The functional aspect is concerned with the functionality of collaborating software components; the operational aspect is concerned with the distribution of components across the organization's geography, in order to achieve the required service level characteristics. A reference architecture is not only a software architecture; it also provides predefined structures for the placement of software on hardware nodes, structures for hardware connectivity, operations and management of the environment. The technical reference architectures are seen as a set of technology

templates based upon a specific architecture paradigm, for example, Service Oriented Architecture (SOA), on which solutions are defined and developed.

One example of a layered-services based technical reference architecture guided by the technical reference model is presented below.

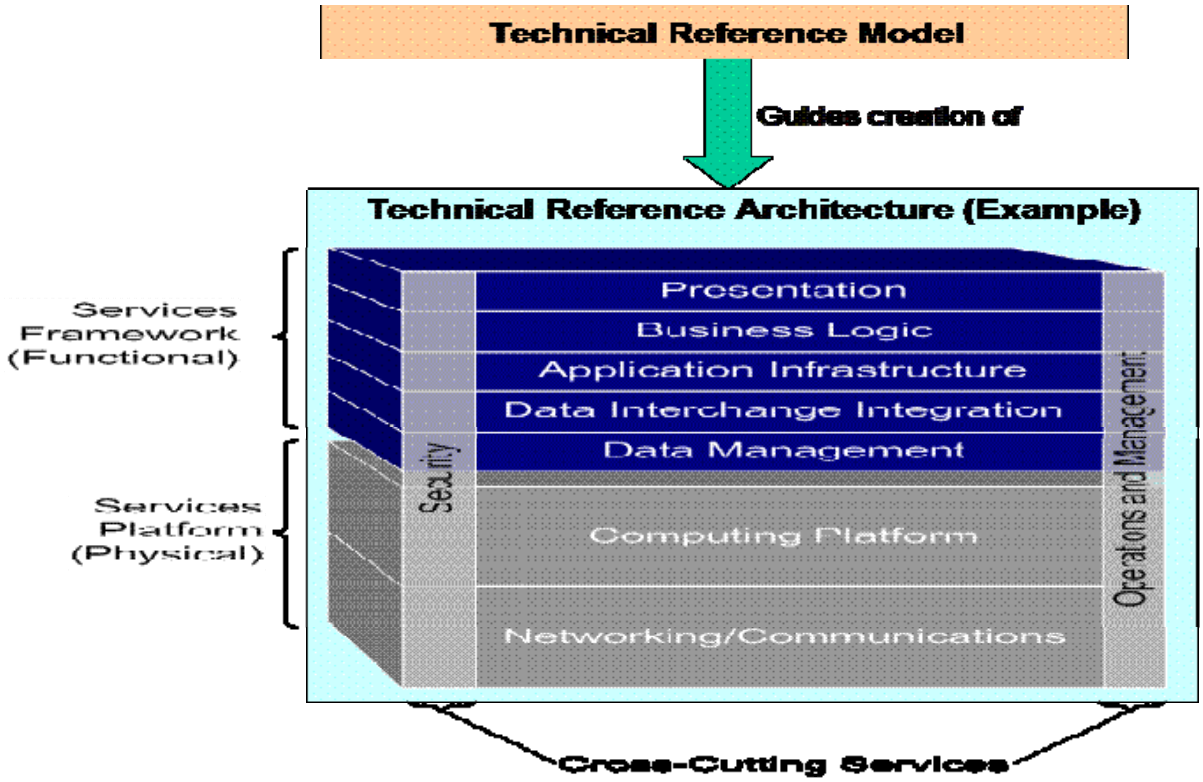


Figure 10 -- Example of a Technical Reference Architecture based upon the Technical Model

This reference architecture features ten architecture service areas or “architecture domains” in a functional layered concept. These architecture domains are:

- Presentation
- Business Logic
- Application Infrastructure
- Data Interchange Integration
- Data Management
- Computing Platform
- Network/Communications
- Security
- Operations and Management

General characteristics of these functional layers are:

- A layer contains logically consistent groupings of services.

- Layers “higher” in the technical reference architecture use the services of those “lower” in the technical reference architecture.
- Services in one layer should not interface with services in other layers except through clearly defined paths.
- Lower levels can be implemented and deployed before higher levels. However, it is difficult to deploy a higher-level layer without the necessary lower-level layers because higher levels depend on the capabilities of lower levels.
- A particular function in a layer does not have to utilize all of that layer’s interfaces
- Layers build in a cumulative fashion. For example, platform services are under-pinned by storage management services, communication services, and the physical environment in which they are housed.

This functional layering approach better reflects the layering of services that exist in current vendor and Open Source products which in turn facilitates definition of solution architecture.

3.0 Standards Profile

A standards profile is a technique of referencing (in contrast to defining) technical specifications (e.g., standards and specifications). A standards profile permits the creation of a set of standards, which provides a common foundation for the realization and implementation of the components defined in the Technical Model. A standards profile is merely a collection of references to standards or specifications, not the definition of the standards wording and description.

Standards profile is developed based upon the Technical Model core taxonomy. It is a database of facts and guidance about information systems standards. The standards to which it refers come from many sources: from formal standards bodies such as ISO or IEEE; from authoritative consortia, like the World Wide Web Consortium and the Object Management Group; and, from internal sources of an agency implementing HR LOB solution.

The HR LOB Standards profile is rooted in the concept of an open systems environment and, through its application, supports portable, scalable, and interoperable applications through standard services, interfaces, data formats, and protocols.

The HR LOB Standards Profile provides insight and guidance in the development of technical and system architectures that satisfy requirements across missions, and in particular where interoperability, reuse, and open systems are desirable. The Standards Profile guides the selection of standards for interfaces, services and products in support of the HR LOB Enterprise Architecture.

3.1 Standards Applicability

Standards and best practices should be adopted and implemented in order to achieve improved interoperability and reuse, overall cost savings and other benefits, including reduction of complexity, and/or assurance of continued availability of service. Exceptions to standards and best practices may be considered only when a non-conforming technology is essential to fulfillment of a unit's role and mission.

The use of standards in different parts of the system result in higher interoperability by creating uniformed ways for example transporting, integrating, present and describe data. When standards are used in systems, it is easier for other systems to establish a common link between the systems. There are different types of standards that can help in the achievement of interoperability in general and specifically syntactic and semantic interoperability. Standard can be broken down into standards for data, metadata, data transformation, data integration, data presentation, data modeling and description language. The use of each of these types of standards helps achieve a part of the overall interoperability goal. The detailed list of standards supporting each service category is included in the Appendix – D.

The primary purpose of these standards is to provide inputs to the architect during the development process to populate the architecture with technologies and products that meet HR LOB requirements. Other use of the standards profile is to help to ensure that the procurement gives a clear statement of technical requirements, with an assurance of conformance during the

procurement of HR LOB solution. The HR LOB standards profile can be categorized into different profile-views based upon service areas, user requirements, and architectural requirements, such as mandatory standards view, common services standards view, portal view, data related standards, and hardware and infrastructure standards. These profile-views group the standards to increase their applicability and usability.

3.2 Mandatory Standards

The standards contained in the TM are based upon commercial open systems technology strongly supported in the commercial marketplace. Following criteria provide guidelines for mandating a standard:

- The standard promotes interoperability;
- The standard demonstrates maturity through technical stability and strong support in the marketplace, and maintenance by a recognized organization;
- The standard can be technically implemented;
- Wide distribution and adoption of the standard demonstrates that it is publicly available (with at least three products openly available);
- The standard is consistent with authoritative sources such as laws, regulations, policy, and guidance documents.

A comprehensive list of mandatory standards for the HR LOB is defined in the profile-view as follows:

- **Legislative and Compliance**
    - **Section 508** -- requires Federal agencies' electronic and information technology is accessible to people with disabilities, including employees and members of the public. It establishes requirements for any electronic and information technology developed, maintained, procured, or used by the Federal government.
    - **Web Content Accessibility** -- W3C Standards (Document Object Model (DOM), HTML, HTTP, CSS, XML, and URI/URL); ISO Web Usability Standards ISO/AWI 23973;
- **Security –** NIST SP 800 Series; Departmental Guide to Network Security
- **Privacy: Platform for Privacy Preferences (P3P**)
- **Security / Authentication / Single Sign-On** - NIST SP 800 Series; FIPS 140-2
- **Hosting**
    - **Internal –** NIST SP 800-40; NIST SP 800-44; NIST SP 800-53;
    - **External – ISP/ASP/First Gov:** Web Page Design Standards
- **Communication Services**
    - **Network Services** – TCP/IP, IPv4, IPv6, Traditional IP Network Address Translator, Mobile IPv4, X.25, Point-to-Point Protocol (PPP), Internet Protocol Control Protocol (IPCP), ISO/IEC 8802-3:2000 (CSMA/CD), RS-232, RS-422, RS-423
    - **File Transfer –** FTP; HTTP; HTTPS, URL, URI
    - **Email –** IMAP, POP3, SMTP, MIME, X.400
    - **EDI –** X.12, UN/EDIFACT, HL7, ISO/IEC 9735:1998, ITU T.120

- **Directory Services –** X.500, DAP, LDAP, SOAP, LDIF, UDDI
- **Domain Name –** DNS (IETF Std 13:1987)
- **Remote Terminal** -- Telnet

3.3 Standards Profile-Views

Many profile-views of HR LOB Standard profile can be defined by organizations implementing HR Lob solution to facilitate standards adoption and usage. This document describes some of the commonly used profiles.

3.3.1 User Portal Standards Profile-View

- **Presentation / Interface**
  - **Static Display** -- Hyper Text Markup Language (HTML); IEEE 1295, FIPS 158-1, XML, ANSI X3.124, ANSI X3.144-1988, ISO 9592-1:1989;
  - **Dynamic Server-side Display** -- Active Server Pages (ASP); JSP, DHTML
  - **Content Rendering** -- HTML; IEEE 1295, FIPS 158-1, XML, ANSI X3.124, SVG, PHIGS, ANSI X3.144-1988, ISO 9592-1:1989;
  - **Wireless/Mobile/Voice** -- ITU Standards G.711, G.722, G.722.1, G.728 for Audio; ITU Standards H.239, T.120 for Data; ITU Standards H.221, H.231, H.242, H.243 for Control
- **Access Channel**
  - **Web Browser** -- W3C Standards (Document Object Model (DOM), HTML, HTTP, CSS, XML, and URI/URL); ISO Web Usability Standards ISO/AWI 23973;
- **Desktop Applications**
  - **Presentation / Publication –** Document Object Model (DOM)
  - **Electronic Forms –** XML- XForms
  - **Drawing** -- ISO 128-21:1997; ISO 13567 Series; ISO 11442 Series; ANSI Y14.5 standards.

3.3.2 Data and Database Standards Profile-View

- **Database** -- ISO/IEC 9579- 2; ISO/IEC SQL:1999; FIPS 193;
- **Storage Devices** -- ANSI/AIIM MS 66-1999; SCSI and iSCSI, FCIP and iFCP, ESCON,
- **Data Warehousing** -- Common Warehouse Metamodel (CWM)
- **Database Connectivity** -- ODBC, JDBC, OLE DB for OLAP, XMLA, LDAP, X.500
- **Data Management** -- OMG's Metadata Standards; Dublin Core; ODMG 3.0;
- **Data Exchange** -- XMI, Xquery, Simple Object Access Protocol (SOAP), X12, UN/EDIFACT, ISO/IEC 9735:1998, PEDI, HL7, ITU-T X435-1997, ebXML, BPEL4WS
- **Database Access** -- ISO/IEC 9579- 2; ISO/IEC SQL:1999; FIPS 193; ODMG 3.0:2000; XML, XSL, XSLT, Xpath, DOM, XBRL 2.0, SGML, XHTML
- **Data Format / Classification** -- XML, NISO Z39.87-2002, AIIM20-2002
- **Data Types / Validation / Transformation** -- Document Type Definition (DTD), XML Schema; eXtensible Stylesheet Language Transform (XSLT)

3.3.3 Application Services Standards Profile-View

- **Web Services –** HTTP, SOAP, MTOM, SOP, WS-Addressing, WSDL, WS-Security
- **File and Print Services** -- NFS, CIFS and SAMBA "shares" ; CORBA 2.0; Direct Access File System (DAFS) Protocol;
- **Application Program Interfaces** -- Java API for XML Registries (JAXR); Web Services Description Language (WSDL); Web services (SOAP/XML) API
- **Enterprise Application Integration** -- JAXM, J2EE Connector Architecture (JCA), OSA-EAI,
- **Transaction Services** -- DTP, ISO/IEC 10026:1998, ISO/IEC 9805:1998, ISO/IEC 12061:1995
- **Middleware** -- Message Oriented Middleware, PolyORB;
- **Business Logic (Programming) –** C, C++, Java, JavaScript, JDK, JSP, Visual C++, Visual Basic, JDK; Visual Basic.NET
- **Transaction Processing –** DTP, ISO/IEC 10026:1998, ISO/IEC 9805:1998, ISO/IEC 12061:1995
- **Transaction Gateways –** Web Services Transaction (WS-Transaction); VoIP Protocols (MGCP, SIP, and ITU H323)
- **Service Discovery / Description / Interface –** WS-Metadata Exchange; URI, UDDI 2.0; Web Services Description Language (WSDL) 1.1; WS-Policy; BEPL4WS

3.3.4 Infrastructure Services Standards Profile-View

- **Hosting –** NIST SP 800-40; NIST SP 800-44; NIST SP 800-53;
- **Support Platforms –**
    - **Platform Independent:** J2EE 1.4; Java APIs for XML; SOAP; JDBC; CORBA; Java 2 Platform; J2EE Connector Architecture;
    - **Platform Dependent:** ASP.NET; VB.NET 2.0; CLR; COM/DCOM/COM+; C# ("C sharp");
- **Network Devices** -- NIST SP 800-46;
- **WAN / LAN** -- IEE 802 series of standards; TCS/TCE
- **Network Services / Transport** -- NIST SP 800-52
- **Internet, Intranet, Extranet, VPN** -- NIST SP 800-52; NIST SP 800-46;
- **Collaboration / Communication** -- NIST SP 800-49; NIST SP 800-45
- **Wireless / Mobile** -- WPA; WPA2; 3GSM; IEEE 802.11N; WAP; UMTS; CWML; GPRS
- **Network Design Tools** -- IEEE 802.1 Q; IEEE 802.1 D
- **Web, Network, FTP, and Backup Services** -- ITU T.120 Standards; SOAP, WSDP; FIPS 140-2; Web services (SOAP/XML) API; UDDI 2.0;

3.3.5 Security Services Standards Profile-View

- **Certificates / Digital Signature –** NIST SP 800-15; NIST SP 800-32; X.509;

- **Encryption –** FIPS 140-2, NIST SP 800-21;
- **Role Definition, Access Control –** NIST SP 800-32; NIST SP 800-25; NIST SP 800-21
- **Audit, Anti-Spam, Anti-Virus –** COBIT, FISCAM, ISO17799
- **Vulnerability Scanning, Penetration Testing –** NIST SP 800-42
- **Firewall, Intrusion Detection –** NIST SP 800-41
- **Security Support Services –** SAML; SSH; SSL; S/MIME; NIST SP 800-49; FIPS 113; FIPS 180-2; FIPS 185; FIPS 186-2; FIPS 197; FIPS 198; WS-Security; SAML
- **Authentication, Single Sign-On –** NIST SP 800-25; NIST SP 800-32; NIST SP 800-56; NIST 800-57; NIST SP 800-63; NIST 800-70; X.509; FIPS 201

3.3.6 Technical Support Services Standards Profile-View

- **Application Management**
    - **Software Configuration Management --** ISO/IEC 12207, ISO 10007:2003, ISO/IEC TR15846, ANSI/IEEE Std 1042-1987; IEE Std 828-1998
    - **Quality Management –** ISO 9001:2000
    - **Testing --** ISO 9001:2000; ISI/IEC 12119; IEEE 730; IEEE 1008; IEEE 1044;
    - **Project Management --** PMI OPM3 Standard;
- **Document Management --** ISO 15489 Series; ISO 15801; AIIM and ARMA Standards
- **Integrated Development Environment –** J2SE SDK; XML IDE***;***
- **Modeling –** UML 1.5, XML, IDEF Series, BPML, CWM, MOF 1.4

3.4 Open Standards

The HR LOB will use only open standards wherever possible when attempting to standardize a service. An Open standard is a standard that is publicly available and has various rights of use associated with it. Open Standards are standards made available to the general public and are developed (or approved) and maintained via a collaborative and consensus driven process. Open Standards facilitate interoperability and data exchange among different products or services and are intended for widespread adoption. Open standards in interoperability issues help to foster processes for quicker integration of components having standardized interfaces and increased automation of common requirements. The more we use and deploy open standards, the greater our vendor independence. Open standards decrease the cost of changing vendors by decreasing the costly components of change, resulting in improved and increased vendor options.

A number of standards organizations create and publish standards that impact the HR LOB Standards profile. The major organizations from which this Standards Profile is derived are as follows:

- American National Standards Institute (ANSI) – ANSI is a voluntary standardization organization whose purpose is to administer and coordinate standardization efforts in the private sector.
- National Institute of Standards (NIST) – NIST, publisher of the Federal Information Processing Standards (FIPS), was formed under the Information Technology Management

Reform Act (Public Law 104-106) and authorizes the Secretary of Commerce to approve standards and guidelines for Federal computer systems.

- IEEE Standards for Computer Engineering – IEEE is a non-profit, technical professional association of more than 377,000 individual members in 150 countries. The IEEE organization publishes a number of standards in a number of technical areas ranging from computer engineering, biomedical technology and telecommunications, to electric power, aerospace and consumer electronics.
- Internet Engineering Task Force (IETF) – The IETF is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It publishes standards that are related to the Internet, its use, and development of applications for the Internet.
- International Standards Organization (ISO) – ISO is a worldwide federation of national standards bodies from some 140 countries, whose mission is to promote the international development of standardization and related activities with a view to facilitating the international exchange of goods and services, and to developing cooperation in the spheres of intellectual, scientific, technological and economic activity. ISO's work results in international agreements, which are published as international standards.
- International Telecommunications Union (ITU) – The ITU is an intergovernmental organization, within which the public and private sectors cooperate for the development of telecommunications. The ITU adopts international regulations and treaties governing all terrestrial and space uses of the frequency spectrum as well as the use of the geo-stationary satellite orbit, within which countries adopt their national legislation. It also develops standards to facilitate the interconnection of telecommunication systems on a worldwide scale regardless of the type of technology used.
- World Wide Web Consortium (W3C) – The W3C's purpose is to develop interoperable technologies (standards, specifications, guidelines, software, and tools) for the Internet.

3.5 Standards Adoption Process

The HR LOB Standards Profile must be kept up-to-date to provide value to organizations and projects providing HR LOB solutions and services. The HR LOB Standards Profile must reflect the impact of the following types of changes:

- **New Technology.** Information systems technology is changing rapidly, often in ways that cannot be predicted. As technology evolves, trends and changes should be monitored, and new products should be evaluated for their applicability to the HR LOB Technical Architecture.

- **New or Revised Standards.** Standards organizations are actively adding to and changing the body of consensus-based standards. The emerging internationalization of information technology standards is further stimulating reconciliation and acceleration of standardization activities. Standards already selected in the HR LOB Standards Profile need to be monitored for changes and obsolescence, while emerging standards should be tracked and assessed regularly for inclusion in the profile.

- **New or Revised User Requirements.** User expectations and needs are primary drivers in determining the services architecture must provide and in selecting products to implement them. In the broad, dynamic environment of organizations implementing HR LOB solution, user requirements evolve quickly. The interoperability demands of users and architecturally-significant mission systems must be evaluated frequently to assess their impact on the HR LOB Technical Model.

4.0 HR LOB Technical Model Traceability

Traceability is the thread that connects the technical model components to the business model components. Traceability links business strategies and information technology. It confirms the technology solution represents the implementation view of the business solution to agreed levels of accuracy. In enterprise architecture, the term traceability (or requirements traceability) refers to the ability to link requirements back to stakeholders' rationales and architecture drivers and forward to corresponding architectural models, artifacts, standards,and technology. Traceability is achieved by creating a semantic relationship between the different reference models (or layers) of the architecture.

Traceability is required:

- To ensure completeness – facilitate the identification of requirements which are not satisfied by the system by following traceability links;
- To propagate the changes - find out the elements impacted by changes at any time in the development process;
- To facilitate mutual understanding and enable semantic interoperability – as a lot of participants with a diverse background come in different development phases;
- To manage information produced during distributed collaborative system development.

Traceability enables forward identification of change or, in other words, the capability to trace the rational thread of impact from the point of origination down to the supporting components of technology. The inverse is also true. A change in technology can also be traced backwards to the driving business process. Traceability also enables the gathering of metrics on business and software completeness by measuring backwards from software code to the originating requirement element.

HR LOB Target CONOPS document dated June 30, 2004 establishes the initial requirements for traceability by defining the target architecture for the HR LOB should be based on the ability to "thread" service components together to support achieving business needs. The HR LOB directly focuses on common business components needed to fulfill agency HR needs. The business service components are implemented using technology service components in the technology layer. Technology service components include such services as data management, workflow, personalization, and scheduling. At the lowest level, the technology infrastructure upon which technology service components execute include such items as hardware, operating systems, and networks. The ability for agencies to select and "thread" appropriate service components is achievable through the use of standardized component interfaces and information exchange mechanisms. The following diagram shows the traceability of the reference model elements.

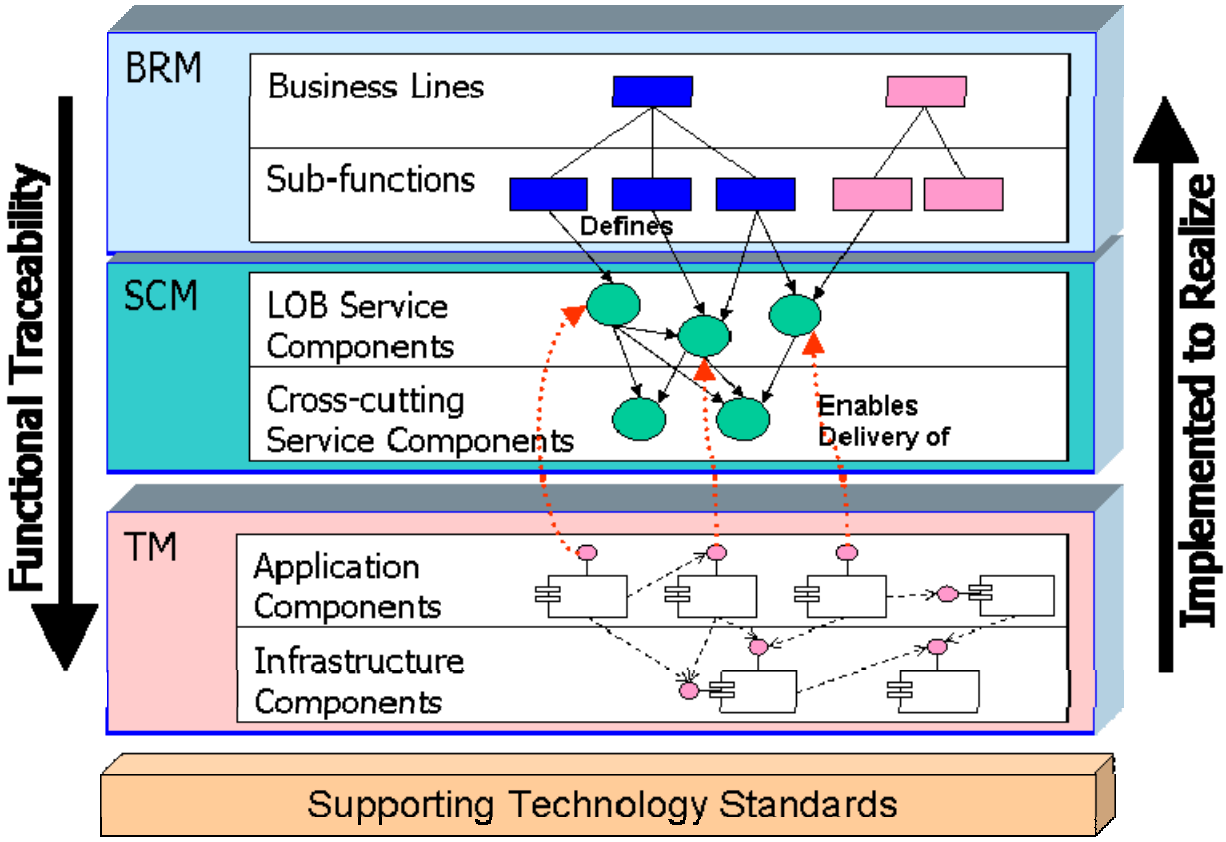


Figure 11 -- HR LOB Technical Model Functional Traceability

HR LOB SRM Mapping document dated June 30, 2004 establishes the traceability between the Business Reference Model (BRM) and the Service Component Model (SCM) by providing the connection between business processes and the business and technical services (components) used to support the business processes. The connection between the Service Component Model (SCM) and the Technical Model (TM) describes the flow of how a service is delivered to the users or user types enabled by the technology.

4.1 TM Traceability to SCM

The HR LOB SCM document defines the service delivery model that recommends *how* each capability, i.e., the Service Component, will be made available to the consumers of the capability. The service delivery model identifies and defines the various consumers of services, or "user types". It maps those users to service components, showing which users use which services. And for each use instance, it proposes the "delivery channel" to be used to deliver the service to the user in an effective and efficient manner. Service delivery channels show the manner in which each service component would be accessed by the users who have access to it.

Typically delivery channels are organized into a tiered structure. The users of each service component gain access at a particular level and may be escalated to successively higher levels as necessary. Tier 0, the Direct Access tier enables the user to perform an action related to the task

or activity without any direct involvement or guidance from another person. This environment provides the capability for managers and employees to directly enter and receive data.

Therefore, the capability defined in a Service Component will be delivered to the user or user type using a Service Delivery Channel enabled by the technology and supported by the standards. The technology and standards are defined in the Technical Model. The linkage between a service component and the technology is captured using flow diagramming technique called "Delivery Process-Action Chain". The following diagram shows the template of the Delivery Process-Action Chain (control flow) diagram.

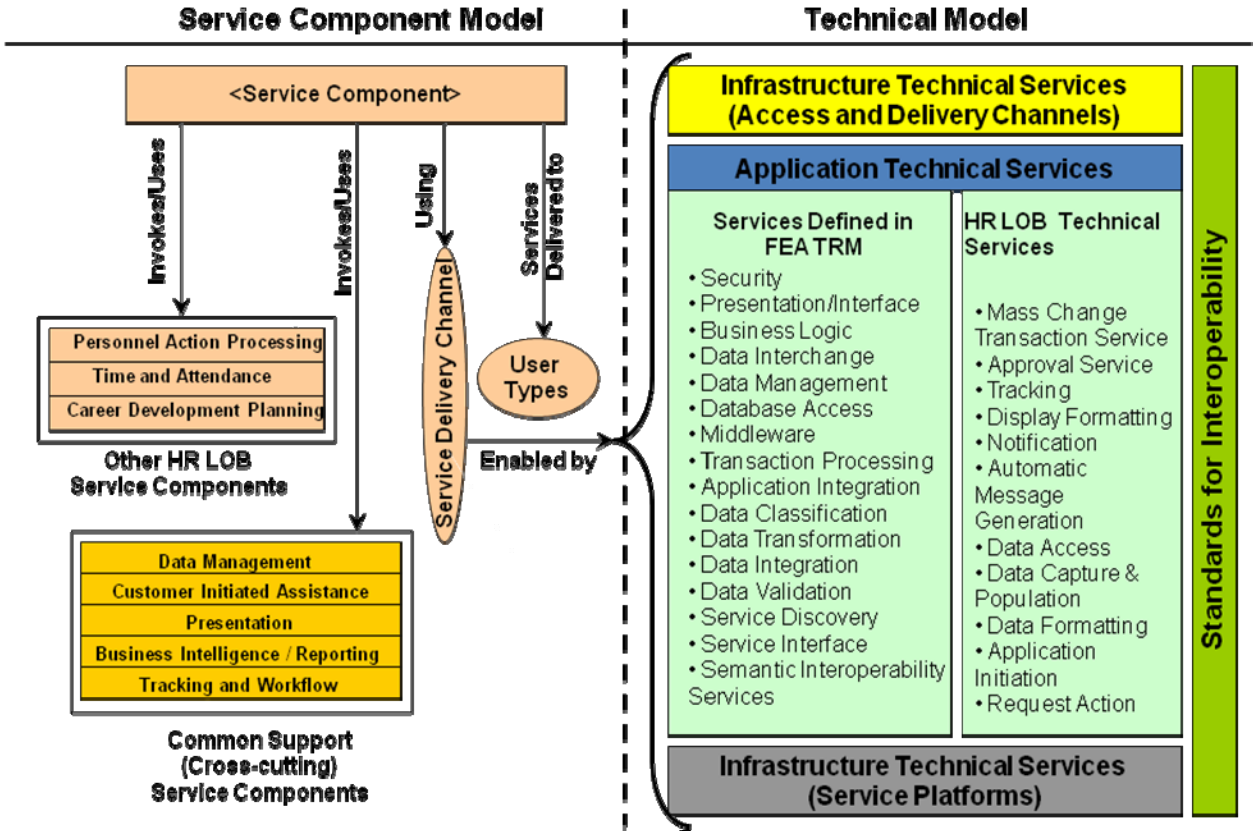


Figure 12 -- Delivery Process-Action Chain (Control Flow) Template

The delivery process-action chain establishes the traceability between the SCM and the TM by providing the details of technology service components (Service Area and Service Category) required to deliver the capability defined by the service component and standards that support the service category. The detailed delivery process-action chain diagrams for each service component defined for the Core HR function is included in the Appendix – A.

4.2 TM Traceability to Requirements

Requirements are a specification of what should be implemented. They are descriptions of how the system should behave, or of a system property or attribute. They may be a constraint on the development process of the system. The business process requirements are the source that determines how and where technology is used in achieving organizational goals. Forward traceability determines the technology components that will facilitate the realization of the requirements. It is also essential to trace the technology model components to the requirements to support impact analysis, i.e., to determine the impact changes in the technology components are going to have on the requirements. A seemingly simple change in a business rule may change the requirements which in turn may have significant impact on the technology that implements those requirements. Without the requirement traceability matrix, it is often not easy to identify the impact, or to understand the extent of the impact once identified.

But traceability can do more. It can also enable the discovery of unrealized requirements. Many times requirements, for one reason or another, are not fully recognized. Traceability maps the route of impact from strategy to process to technology and back again. Along this route, requirements that are often obscured by business or technology complexity will be revealed.

There are over 450 requirements defined for the HR LOB that cover three areas of "Core HR": Personal Actions, Benefits, and Compensation. These requirements were used as the primary source for identification of "specialized" technical services applicable to HR LOB (not defined in the FEA TRM). This following diagram shows an example (one page) of the requirements traceability matrix. It means, for example,

- PPA 82 and PPA 83 – Requirement specifies for the initiation of a Personal action by Users
- This requires a special Technical Service – **Initiation Service** (first column)
- This Initiation Service Initiation Service
    - detects transactional **Event** (customer data is accessed, updated, or added) or non-transactional **Event** (e.g., date driven events);
    - identifies the user action;
    - triggers the data validation based upon business rules,
    - triggers the request for appropriate transaction

Requirement #	Requirement Priority	Requirements HR LOB Technical Services ==>>	Initiation / Request Action Services	Mass Change Transaction Services	Tracking Service	Approval Services	Notification	Automatic Message Generation	Data Access	Data Validation	Data / Display Formatting	Data Capture / Population	Data Integration
PPA45	M	Obtain signatures in support of Personnel Actions IAW the Guide to Processing Personnel Actions				X							
PPA46	M	Obtain approvals for Personnel Actions IAW the Guide to Processing Personnel Actions				X							
PPA47	M	Obtain approvers for Personnel Actions IAW the Guide to Processing Personnel Actions				X							
PPA48	M	Obtain all required documents for Personnel Actions IAW the Guide to Processing Personnel Actions											
PPA80	M	Move candidate data to employee data upon entry of the appointment personnel action							X				
PPA81	M	Automatically delete the WGI due date when an employee converts from a permanent to a temporary appointment							X				
PPA82	M	Allow users to initiate personnel actions in a secure automated solution	X										
PPA83	C	Allow users to initiate personnel actions in a secure automated Web-based solution	X										
PPA84	M	Allow users to edit personnel action data to a secure automated solution								X			
PPA85	C	Allow users to edit personnel action data to a secure automated Web-based solution								X			
PPA86	M	Information displayed will be tailored to the role of the user. (Roles will be defined)								X			
PPA87	M	Facilitate completion of online personnel action through menu-driven drop down boxes and lists of values with descriptions; values may vary by action											
PPA88	M	Pre-populate existing applicable employee information							X	X			
PPA89	M	Pre-populate position data							X	X			

Figure 13 -- Example of HR LOB Requirements Mapping to Technical Services

Detailed matrices mapping requirements to technical service components have been included in Appendix – B.

5.0 Conclusion

Historically, the U.S. Federal Government has taken an agency-centric approach to delivering human resources services to government employees. Agencies have their own human resources (HR) missions, HR staffs, HR management practices and technology. Many organizations continue to buy or re-create similar, if not identical, functionality across different applications. The management of such separated functions has resulted in sub-optimal support for business processes, and additional costs to the organization.

The HR LOB Technical Model and the Best Practices Reference, is intended to form a knowledge-base to provide a common conceptual framework, and define a common vocabulary and a set of services and interfaces that are, or will be, common to HR LOB systems. The technical model provides the foundation to advance the re-use of technology and component services across HR LOB and the Federal Government through standardization. The *Technical Model* influences all aspects of the *Enterprise Architecture*. It provides the enabling forces for a high level of design integrity in the areas of interoperability, extensibility, scalability, re-usability, portability, security, reliability, and performance. While the HR LOB TM is a powerful model that provides a vendor-neutral, open-standard definition of technical service components, its abstract nature means further work must be done to create reference architecture.

Federal agencies, just like any other global enterprise, are now at a crossroads for establishing an SOA strategy, in a world where no single strategy can possibly cover every need. SOA is a driving force for future functional use within organizations. However, these functions must be viewed as being shared services for all processes. Functional re-use will be the main means of ensuring organizations can respond rapidly and effectively to market dynamics, and improvements to specific functions will have the optimum impact across the whole organization. The HR LOB Technical Model will guide the development of HR solution architecture based on SOA paradigm; in selecting the protocols, profiles, specifications, and standards are suitable for solution; and requirements, motivations, and goals are taken into account.

The Technical Model is not intended to provide or endorse particular vendor products. It is a living document that will be modified to reflect the needs of HR LOB and the rapid changes occurring in information technology.

Appendix

Appendix – A Technical Service traceability to SCM components

Please contact HR LOB at hrlob@opm.gov for the Delivery Process-Action Chain Diagram – Technical Model Structure for the following sub-functions:

1) Employee Self-Service
2) Manager Self-Service
3) Personnel Action Processing
4) Time and Attendance
5) Payroll/Benefits Processing
6) Payroll/Benefits Reporting
7) Position Classification
8) Recruiting and Application Management

Appendix – B Requirements Mapping to Technical Services

Please contact HR LOB at hrlob@opm.gov for the Requirements Mapping to the following Technical Services:

1) Service Access and Delivery Services
2) Service Platform and Infrastructure Services
3) Component Framework Services
4) Service Interface and Integration Services
5) HR LOB Specific Technical Services

Appendix – C Abbreviations and Acronyms

ANSI	American National Standards Institute
API	Application Program Interface
ARPA	Advanced Research Projects Agency
ASCII	American Standard Code for Information Interchange
ASP	Active Server Pages
BPEL	Business Process Execution Language
BRM	Business Reference Model
CAD	Computer-Aided Design
CAE	Common Applications Environment
CAM	Computer-Aided Manufacturing
CASE	Computer-Aided Software Engineering
CDIF	CASE Data Interchange Format
CGI	Common Gateway Interface
CGM	Computer Graphics Metafile
COBIT	Control Objectives for Information and related Technologies
COBOL	Common Business Oriented Language
CORBA	Common Object Request Broker Architecture
CSS	Cascading Style Sheets
DAA	Data Authentication Algorithm
DAP	Directory Access Protocol
DCE	Distributed Computing Environment
DDF	Data Descriptive File
DES	Data Encryption Standard
DMA	Document Management Alliance
DNS	Domain Name System
DOM	Document Object Model
DRM	Data Reference Model
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
DTD	Document Type Definition
DTE	Data Terminal Equipment
EA	Enterprise Architecture
ECMA	European Computer Manufacturers Association
EDI	Electronic Data Interchange
EIA	Electronics Industry Association
EJB	Enterprise Java Beans
ESB	Enterprise Service Bus
EMPM	Electronic Manuscript Preparation and Markup
FEA	Federal Enterprise Architecture
FEAF	Federal Enterprise Architecture Framework
FIPS	Federal Information Processing Standards
FISCAM	Federal Information Systems Control Audit Manual
FTP	File Transfer Protocol

FTR	Federal Telecommunications Recommendation
FTSC	Federal Telecommunications Standards Committee
GIF	Graphical Interface Format
GILS	Government Information Locator Service
GIS	Geographic Information System
GKS	Graphical Kernel System
GSSAPI	Generic Security Service API
GUI	Graphical User Interface
HDF	Hierarchical Data Format
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IETF	Internet Engineering Task Force
IGES	Initial Graphics Exchange Specification
IIOP	Internet Inter-ORB Protocol
IM	Instant Messaging
IMAP	Internet Message Access Protocol
IP	Internet Protocol
IPSec	Internet Protocol Secure
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
IT	Information Technology
ITU	International Telecommunications Union
IVR	Interactive Voice Response
J2EE	Java 2 Platform Enterprise Edition
JBI	Java Business Integration
JDBC	Java™ Database Connectivity
JPEG	Joint Photographic Experts Group
JTC	Joint Technical Committee
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LDAP	Lightweight Directory Access Protocol
MIME	Multipurpose Internet Mail Extensions
MOSS	MIME Object Security Services
MPEG	Moving Pictures Experts Group
MTOM	Message Transmission Optimization Mechanism
NETCDF	Network Common Data Form
NISO	National Information Standards Organization
NIST	National Institute of Standards and Technology
OASIS	Organization for the Advancement of Structured Information Standards
ODA	Open Document Architecture
ODBC	Open Database Connectivity
OLAP	Online Analytical Processing
OLB	Object Language Binding
OMG	Object Management Group

OMT	Object Modeling Techniques
OO	Object-Oriented
OSE	Open Systems Environment
OSF	Open Software Foundation
OSI	Open Systems Interconnection
OWL	Web Ontology Language
PDA	Personal Digital Assistant
PDF	Portable Document Format
PHIGS	Programmer's Hierarchical Interactive Graphics System
PKI	Public Key Infrastructure
POP3	Post Office Protocol 3
POSIX®	Portable Operating Systems Interface
PRM	Performance Reference Model
PSTN	Public Switched Telephone Network
RDF	Resource Description Framework
RPC	Remote Procedure Call
RTF	Rich Text Format
SAML	Security Assertion Markup Language
SCSI	Small Computer Systems Interface
SGML	Standard Generalized Markup Language
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
SP	Standards Profile
SQL	Structured Query Language
SQL-J	Structured Query Language - Java™
SRM	Service Reference Model
SSL	Secure Sockets Layer
STEP	Standard for the Exchange of Product Model Data
TCP	Transmission Control Protocol
TDEA	Triple Data Encryption Algorithm
TIA	Telecommunications Industry Association
TIFF	Tagged Image File Format
TLS	Transport Layer Security
TRM	Technology Reference Model
UDDI	Universal Description, Discovery, and Integration
UML	Unified Modeling Language
URL	Uniform Resource Locator
VPN	Virtual Private Network
WAN	Wide Area Network
W3C	World Wide Web Consortium
WML	Wireless Markup Language
WSDL	Web Services Definition Language
WSRP	Web Services for Remote Portlets
WSUI	Web Services User Interface

WWW	World Wide Web
XDS/XOM	X/Open Directory Service X/Open OSI Abstract Data Manipulation
XFN	X/Open Federated Naming
XHTML	Extensible Hypertext Markup Language
XMI	XML Metadata Interchange
XML	Extensible Markup Language
XMLA	XML for Analysis
XOP	XML-binary Optimized Packaging

Appendix – D Detailed list of Standards applicable to Service Category

Service Category: Access Channels

Service Subcategory	Specification /Technology	Standards
Collaboration Communications	Electronic Mail (E-Mail)	Simple Mail Transfer Protocol (SMTP); Extended SMTP (ESMTP); Secure/Multipurpose Internet Mail Extensions (S/MIME)
	Facsimile (Fax)	ITU-U Recommendations: T-6, T-30, T-60, T-61, T-62, T-62bis, T-70, T-72, T-73, T-503, T-521, T-523, and F-161
Other Electronic Channels	Markup Languages	Extensible HyperText Markup Language (XHTML); HyperText Markup Language (HTML)
	Voice Protocols	Session Initiation Protocol (SIP)
	Web Services	Asynchronous Service Access Protocol (ASAP); Business Process Execution Language (BPEL); DIME, EbXML; XML; Security Assertion Markup Language (SAML); Simple Object Access Protocol (SOAP); SOAP Message Transmission Mechanism (SOAP MTOM), Universal Business Language (UBL); Universal Description, Discovery, and Integration (UDDI), WS-*
	Web Services – IM/Web Chat	Extensible Messaging and Presence Protocol (XMPP); IRC; Protocol for Synchronous Conferencing (PSYC); Session Initiation Protocol for Instant Messaging and Presence Leveraging Extensions (SIMPLE); Wireless Village (WV)
Web Browser	Browser	DHTML; XHTML; HTML; HyperText Transfer Protocol (HTTP); HTTP Secure (HTTPS)
Wireless/PDA	WPDA	CDMA One; CDMA2000 1xEV-DO; CDMA 1xEV-DV; IEEE 802.15; W-CDMA, Wired Equivalent Privacy (WEP)
	WLAN	IEEE 802.11g; IEEE802.16
	RFID	JTC 1/SC 31 Automatic Identification and Data Capture Techniques JTC 1/SC 17; ANSI/NCITS T6 256-2001

Service Category: Delivery Channels

Service Subcategory	Specification /Technology	Standards
Extranet	WWW	Dynamic HTML; Extensible Markup Language (XML); SOAP; UDDI; Web Services Description Language (WSDL)
Internet	WWW	DHTML; XML; HTML; SOAP; UDDI; WSDL
Intranet	WWW	DHTML; XML; HTML; SOAP; UDDI; WSDL
Peer to Peer (P2P)	Peer to Peer	JXTA; SOAP
Virtual Private Network (VPN)	Hybrid VPN – Secure/Trusted	Layer 2 Tunneling Protocol (L2TP); Secure Socket Layer (SSL); Transport Layer Security (TLS) Protocol

Service Category: Service Requirements

Service Subcategory	Specification /Technology	Standards
Authentication / Single Sign-on (SSO)	Security	FIPS 201; Kerberos; S/MIME; SAML; X.509; XML – Signature Syntax and Processing
Legislative and Compliance	Section 508	Electronic and Information Technology Accessibility Standards (EITAS)
	Security	FIPS 186

Service Category: Service Transport

Service Subcategory	Specification /Technology	Standards
Service Transport	Transport	File Transfer Protocol (FTP); Internet Control Message Protocol (ICMP); IPv6; RMI; SSH File Transfer Protocol (SFTP); Transmission Control Protocol (TCP); User Datagram Protocol (UDP)
Supporting Network Services	Networking	Border Gateway Protocol Version 4 (BGP-4); X.500, Domain Name System (DNS); Dynamic Host Configuration Protocol for IPv6 (DHCPv6); Extended SMTP (ESMTP); Internet Message Access Protocol (IMAP); Lightweight Directory Access Protocol (LDAP); MIME; SMTP; SNMP v3.0; T-120

Service Category: Support Platforms

Service Subcategory	Specification /Technology	Standards
Platform	VMWare	VMWare ESX Server; VMWare Workstation

Independent: Virtualization Platforms		
Platform Independent: Application Support Platforms	Java 2 Platform Enterprise Edition (J2EE)	J2EE 1.4
Platform Independent: Operating Systems	Linux; Unix	Linux; Solaris 10; Unix98
Programming Languages		C#; C/C++; Java; JavaScript; Perl; VBScript; Visual basic.NET, Java 2 Platform;

Service Category: Delivery Servers

Service Subcategory	Specification /Technology	Standards
Application Servers	Application Server	Java 2 Platform Enterprise Edition (J2EE); Linux; Solaris 10; Unix98; JBoss
Media Server		Java 2 Platform Enterprise Edition (J2EE); Linux; Solaris 10; Unix98; • VoiceXML 2.0 speech/IVR media; VoiceXML 2.1 extensions ; CCXML 1.0 call control; SRGS 1.0 speech grammars; SSML 1.0 speech markup; SISR speech semantic interpretation; XML 1.1 and Namespaces in XML 1.1; XML DOM; XPath; Voice XML Standards;
Portal Server		W Java 2 Platform Enterprise Edition (J2EE); Linux; Solaris 10; Unix98; Wireless Markup Language (WML), HTML, Compact HTML (cHTML), eXtensible HTML (xHTML), or Handheld Device Markup Language (HDML) - or platform, including Palm, iPAQ, RIM, Wireless Application Protocol (WAP); Web Services for Remote Portlets (WSRP); JBoss; Java Portlet API
Web Server		HTTP; 40- or 128-bit SSL (RC2, RC4, DES); FTP tools; XML, WML, CGI / FastCGI; ISAPI, NSAPI, and WSAPI; Active Server Pages (ASP)

Service Category: Database / Storage

Service Subcategory	Specification /Technology	Standards
Database	Relational Database	SQL 3 (ISO/IEC 9075(-1 to -14):2003); SQL92; T-

		SQL; JDBC; SQLJ; SQL:1999; Java Data Objects (JDO); ODMG 3.0
Storage	NAS	CIFS; EXT2/EXT3; NTFS
	SAN	Fiber Channel; iSCSI

Service Category: Hardware / Infrastructure

Service Subcategory	Specification /Technology	Standards
Embedded Technology Devices	PDA; Pocket PC, Smart Phone; Processors; Multimedia;	Video Codec: H.264, H.263, H.261, MPEG-4 ASP, MJPEG , MPEG-1, MPEG-2 Audio Codec: MPEG Audio, MP1, MP2, MP3, non-ISO MPEG-2.5, AAC/AAC plus Ogg Vorbis, WMA9, HILN, MPEG-4 Parametric Audio Coding Voice - G.7XX (G.711, G.723, G.726, G.728, G.729), AMR, EFR Image Processing - JPEG, JPEG2000 Automation: Modbus, CAN, Profibus and several proprietary Automotive: CAN - J1587, J1708, J1939, LIN, CCP, OBD2, KWP2000, MOST, D2B Encryption standards and algorithms**:** AES, DES, RSA, SHA Section 508: Technical Standards 1194.24 and 1194.25
LAN	Ethernet 802.3	VLAN IEEE 802.1Q; SNMPv1 (IETF Std 15); LAN/MAN-Overview of LAN standards (ISO/IEC TR 8802-1:97)
WAN		CMIS (ISO 9595:1998)
Video Conferencing		Video Conferencing Standards family (H.320, H.321, H.323, H.324, and H.310), Data Collaboration Standards family T.120

Service Category: Security

Service Subcategory	Specification /Technology	Standards
Certificates / Digital Signature		FIPS 140-2; Internet Key Exchange (IKE); Internet X.509; Keyed-Hash Message Authentication Code (HMAC)
Supporting Security Services		Domain Name System security Extensions (DNSSEC); FIPS 113 (DAA); FIPS 180-2 (SHS); FIPS 185 (EES); FIPS 186-2(DSS); FIPS 197 (AES); FIPS 198 (HMAC); FIPS 201 (PIV); FIPS 46-3 (DES); FIPS 81 (DES); Web Services

		Security Version 1.0

Service Category: Presentation and Interface

Service Subcategory	Specification /Technology	Standards
Wireless / Mobile / Voice		Wireless Markup Language (WML)
Content Rendering	Web Portals	Action Script; AJAX; Cascading Style Sheets (CSS); Java Portlet API (JSR 168); Web Services for Remote Portlets (WSRP)
Dynamic Server Side Display		Active Server Pages; Java Server Pages; Web Service User Interface (WSUI);
Static Display		xHTML; HTML;

Service Category: Data Interchange

Service Subcategory	Specification /Technology	Standards
Data Exchange	Data Format	Dublin Core Metadata Standard; ebXML; SOAP; XML Metadata Interchange (XMI); HTTP v. 1.1; URL; URI; LDAP Data Interchange Format(LDIF);
	File Transfer	Compact Disc File System (CDFS) (ISO 9660:1988); FTP (IETF STD 9:1985)
	Business Transaction Oriented Data Exchange	EDIFACT (ISO 9735:2002); ebXML Messaging Service v.2:2002 (OASIS);
	Page Description or display languages	PDF-Format 1.4
	Office automation Interchange formats	Rich Text Format (RTF); ASCII Text; ISO 646:1991; Document Object Model (DOM) Level 2

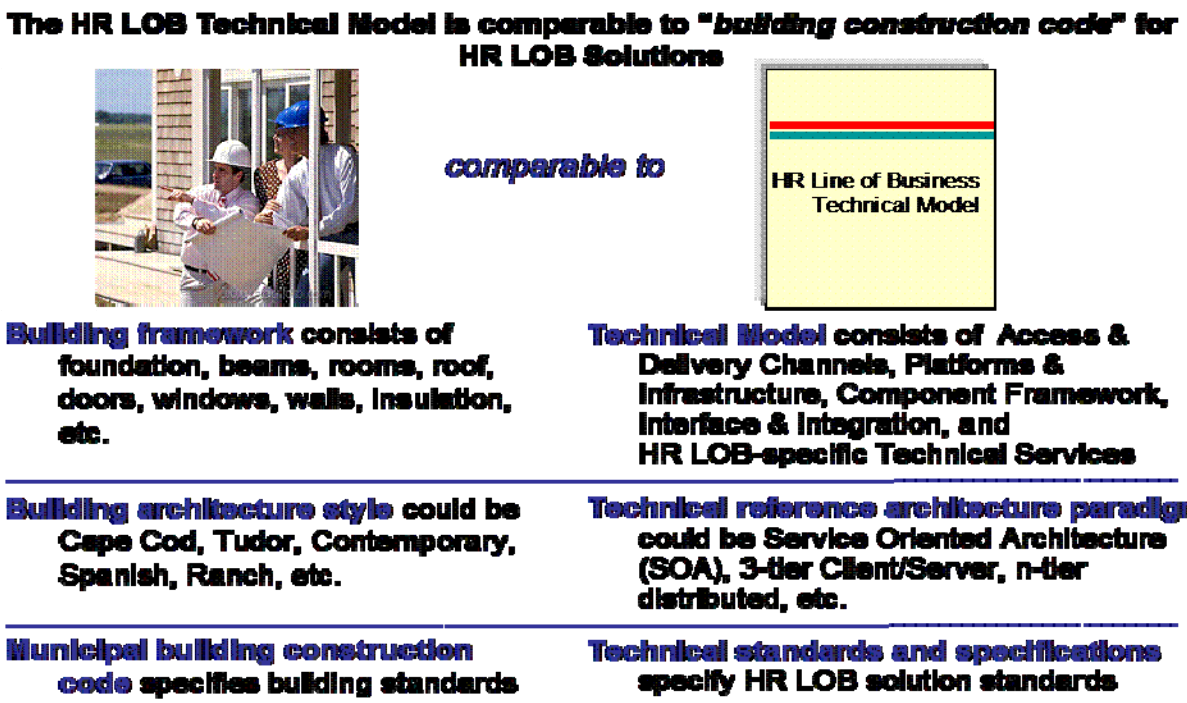
Service Category: Data Management

Service Subcategory	Specification /Technology	Standards
Database Connectivity		ActiveX Data Objects (ADO); ActiveX Data Objects for Data Definition Language and Security (ADOX); Java Data Objects (JDO); Java Database Connectivity (JDBC); OLE/DB; Open Database Connectivity ODBC 3.0 (ISO/IEC 9579:2000); SQL*NET; SQLJ
Reporting and Analysis		JOLAP; XBRL; XML/A; XQuery

Service Category: Integration

Service Subcategory	Specification /Technology	Standards
Enterprise Application Integration	Application Connectivity	XML; Java Message Service (JMS); SOAP; JSR-170
	Business Process Management	BPEL; Java Business Integration (JBI JSR 208)
Middleware	Java 2 Platform (J2EE)	Java EE Connector Architecture (JCA); Java Naming and Directory Interface (JNDI);
	Others	XML-RPC; Integrated Object Model (IOM)

Appendix – E HR LOB Technical Model as the "Building Construction Code"



The HR LOB Technical Model can be used by the Agencies, or Service Centers as a reference for developing a Technical Reference Architecture for the HR LOB Solution Suitable for their requirements.

United States
Office of Personnel Management
1900 E Street, NW
Washington, DC 20415

HRLOB-TM-200801