Solution Architecture - IRDA Business Analytics Project

Nov

2010

Table of Contents

List of Abbreviations Used with Their Definition

Abbreviations	Description
ACL	An access control list (ACL) is a list of permissions attached to an object. An ACL specifies which users--or system processes--are granted access to objects, as well as what operations are allowed to be performed on given objects.
ADS	Active Directory Server (ADS) is a technology created by Microsoft that provides a variety of network services
ANSI	The American National Standards Institute (ANSI) is a private non-profit organization that oversees the development of voluntary consensus standards for products, services, processes, systems, and personnel in the United States
API	An application programming interface (API) is an interface implemented by a software program to enable interaction with other software
ATI	Agent Training Institutes
B2B	Business - to - Business
BCP	Business continuity planning (BCP) is the creation and validation of a practiced logistical plan for how an organization will recover and restore partially or completely interrupted critical (urgent) functions within a predetermined time after a disaster or extended disruption. The logistical plan is called a business continuity plan.
CBAC	Context-based access control (CBAC) intelligently filters TCP and UDP packets based on application layer protocol session information and can be used for intranets, extranets and internets.
CDC/DC	Centralized Data Center or Data Center is a facility used to house computer systems and associated components, such as telecommunications and storage systems.
COM	COM (hardware interface) (COM) is a serial port interface on IBM PC-compatible computers running Microsoft Windows or MS-DOS
DD	Deputy Director
DMZ	The Demilitarized Zone (DMZ) is a critical part of a firewall: it is a network that is neither part of the un trusted network, nor part of the trusted network
DNS	The Domain Name System (DNS) is a hierarchical naming system for computers, services, or any resource connected to the Internet or a private network
DRC	A Disaster Recovery Center (DRC) is a backup site is a location where an organization can easily relocate following a disaster, such as fire, flood, terrorist threat or other disruptive event.
DRM	Disaster Recovery Management (DRM) is the process, policies and procedures related to preparing for recovery or continuation of technology infrastructure critical to an organization after a natural or human-induced disaster.
DTLS	The Datagram Transport Layer Security (DTLS) protocol provides communications privacy for datagram protocols.

Abbreviations	Description
DW	A data warehouse (DW) is a repository of an organization's electronically stored data. Data warehouses are designed to facilitate reporting and analysis
EAI	Enterprise Application Integration (EAI) is defined as the use of software and computer systems architectural principles to integrate a set of enterprise computer applications.
ED	Executive Director
ESB	An enterprise service bus (ESB) consists of a software architecture construct which provides fundamental services for complex architectures via an event-driven and standards-based messaging-engine (the bus).
ETL	Extract, transform, and load (ETL) is a process in database usage and especially in data warehousing
F&A	Finance and Accounts
GUI	A graphical user interface (GUI) is a type of user interface item that allows people to interact with programs in more ways than typing such as computers; hand-held devices etc.
HIDS	A host-based intrusion detection system (HIDS) is an intrusion detection system that monitors and analyses the internals of a computing system rather than the network packets on its external interfaces
HRMS	Human Resource Management System
HSRP	Hot Standby Router Protocol (HSRP) is a Cisco proprietary redundancy protocol for establishing a fault-tolerant default gateway
IDM	Identity management (IDM) is a broad administrative area that deals with identifying individuals in a system (such as a country, a network or an organization) and controlling the access to the resources in that system by placing restrictions on the established identities
JDBC	Java Database Connectivity (JDBC) is an API for the Java programming language that defines how a client may access a database. It provides methods for querying and updating data in a database
LAN	A local area network (LAN) is a computer network covering a small physical area, like a home, office, or small group of buildings
LDAP	The Lightweight Directory Access Protocol (LDAP) is an application protocol for querying and modifying directory services running over TCP/IP
MAC	Mandatory access control (MAC) refers to a type of access control by which the operating system constrains the ability of a subject or initiator to access or generally perform some sort of operation on an object or target
MDM	Master Data Management (MDM) comprises a set of processes and tools that consistently defines and manages the non-transactional data entities of an organization
NIC	Network Information Center (NIC), is the part of the Domain Name System (DNS) of the Internet that keeps the database of domain names, and generates the zone files which convert domain names to IP addresses
ODBC	Open Database Connectivity (ODBC) provides a standard software API method for using database management systems (DBMS)

Abbreviations	Description
ODS	An operational data store (ODS) is a database designed to integrate data from multiple sources to make analysis and reporting easier
OLAP	Online analytical processing (OLAP) is an approach to quickly answer multi-dimensional analytical queries
RBAC	Role-based access control (RBAC) is an approach to restricting system access to authorized users.
RPC	Remote procedure call (RPC) is an Inter-process communication technology that allows a computer program to cause a subroutine or procedure to execute in another address space (commonly on another computer on a shared network) without the programmer explicitly coding the details for this remote interaction.
RPO	Recovery Point Objective (RPO) is the point in time to which you must recover data as defined by your organization. This is what an organization determines is an "acceptable loss" in a disaster situation.
RTO	Recovery Time Objective (RTO) is the duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity.
SAML	Security Assertion Markup Language (SAML) is an XML-based standard for exchanging authentication and authorization data between security domains, that is, between an identity provider (a producer of assertions) and a service provider (a consumer of assertions)
SAN	A Storage area network (SAN), an architecture to attach remote computer storage devices to servers in such a way that the devices appear as locally attached to the operating system
SIP	The Session Initiation Protocol (SIP) is a signaling protocol, widely used for controlling multimedia communication sessions such as voice and video calls over Internet Protocol (IP)
SLA	Service Level Agreement (SLA) is a part of a service contract where the level of service is formally defined. SLA is sometimes used to refer to the contracted delivery time (of the service) or performance.
SOAP	SOAP, originally defined as Simple Object Access Protocol, is a protocol specification for exchanging structured information in the implementation of Web Services in computer networks.
SQL	SQL (Structured Query Language) is a database computer language designed for managing data in relational database management systems (RDBMS)
SSL	Secure Sockets Layer (SSL) is a cryptographic protocol that provides security for communications over networks such as the Internet
SSO	Single sign-on (SSO) is a property of access control of multiple, related, but independent software systems
TAT	Turn Around Time
TCP	The Transmission Control Protocol (TCP) is one of the core protocols of the Internet Protocol Suite.

Abbreviations	Description
TLS	Transport Layer Security (TLS) is a cryptographic protocol that provides security for communications over networks such as the Internet
TPA	Third Party Agents
UDP	The User Datagram Protocol (UDP) is one of the core members of the Internet Protocol Suite, the set of network protocols used for the Internet.
UML	Unified Modeling Language (UML) is a standardized general-purpose modeling language in the field of software engineering.
VoIP	Voice over Internet Protocol (VoIP) is a general term for a family of transmission technologies for delivery of voice communications over IP networks such as the Internet or other packet-switched networks.
VPN	A virtual private network (VPN) encapsulates data transfers between two or more networked devices not on the same private network so as to keep the transferred data private from other devices on one or more intervening local or wide area networks.
WAN	A wide area network (WAN) is a computer network that covers a broad area (i.e., any network whose communications links cross metropolitan, regional, or national boundaries
XML	XML (Extensible Markup Language) is a set of rules for encoding documents electronically

List of Terms Used with Their Definition

Terms	Description
Application Server	An application server is a software framework dedicated to the efficient execution of procedures (programs, routines, scripts) for supporting the construction of applications.
Audit logging	Audit log is a chronological sequence of audit records, each of which contains evidence directly pertaining to and resulting from the execution of a business process or system function.
Biometrics	Biometrics comprises methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits.
Business Intelligence	Business Intelligence (BI) refers to computer-based techniques used in spotting, digging-out, and analyzing business data, such as sales revenue by products and/or departments or associated costs and incomes.
Business process management	Business process management (BPM) is a management approach focused on aligning all aspects of an organization with the wants and needs of clients.
Caching/cache	a cache is a component that improves performance by transparently storing data such that future requests for that data can be served faster. The data that is stored within a cache might be values that have been computed earlier or duplicates of original values that are stored elsewhere.
Conceptual data model	A conceptual data model is a map of concepts and their relationships. This describes the semantics of an organization and represents a series of assertions about its nature.
Content Management	Content management, or CM, is the set of processes and technologies that support the collection, managing, and publishing of information in any form or medium. In recent times this information is typically referred to as content or, to be precise, digital content.
Context based access	Context-based access control intelligently filters TCP and UDP packets based on application layer protocol session information and can be used for intranets, extranets and internets

Terms	Description
Data Encryption	Data encryption is the process of transforming information (referred to as plaintext) using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key.
Data Integrity	Data integrity is data that has a complete or whole structure. All characteristics of the data including business rules, rules for how pieces of data relate dates, definitions and lineage must be correct for data to be complete.
Data Mapping	Data mapping is the process of creating data element mappings between two distinct data models.
Data Profiling	Data profiling is the process of examining the data available in an existing data source and collecting statistics and information about that data.
Database Index	A database index is a data structure that improves the speed of data retrieval operations on a database table at the cost of slower writes and increased storage space.
Database Server	A database server is a computer program that provides database services to other computer programs or computers, as defined by the client–server model.
Digital Signature	A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, and that it was not altered in transit.
Digitization	Digitization is the representation of an object, image, sound, document or a signal (usually an analog signal) by a discrete set of its points or samples.
Firewall	A firewall is a part of a computer system or network that is designed to block unauthorized access while permitting authorized communications.
FTP	File Transfer Protocol (FTP) is a standard network protocol used to copy a file from one host to another over a TCP/IP-based network, such as the Internet.

Terms	Description
Knowledge Management	Knowledge management (KM) comprises a range of strategies and practices used in an organization to identify, create, represent, distribute, and enable adoption of insights and experiences. Such insights and experiences comprise knowledge, either embodied in individuals or embedded in organizational processes or practice
Load Balancing	Load balancing is a technique to distribute workload evenly across two or more computers, network links, CPUs, hard drives, or other resources, in order to get optimal resource utilization, maximize throughput, minimize response time, and avoid overload.
Metadata management	Meta-data Management involves storing information about other information. With different types of media being used references to the location of the data can allow management of diverse repositories.
MIS	A management information system (MIS) is a system or process that provides information needed to manage organizations effectively
Multifactor authentication	Multi-factor authentication means two or more of the authentication factor required for being authenticated.
Operational Data Store	An operational data store (or "ODS") is a database designed to integrate data from multiple sources to make analysis and reporting easier.
Payment Gateway	A payment gateway is an e-commerce application service provider service that authorizes payments for e-businesses, online retailers, bricks and clicks, or traditional brick and mortar. It is the equivalent of a physical point of sale terminal located in most retail outlets.
Physical Data Model	A physical data model (database design) is a representation of a data design which takes into account the facilities and constraints of a given database management system.
Portlets	Portlets are pluggable user interface software components that are managed and displayed in a web portal. Portlets produce fragments of markup code that are aggregated into a portal page.
Proxy Server	A proxy server is a server (a computer system or an application program) that acts as an intermediary for requests from clients seeking resources from other servers.

Terms	Description
Role based access	Role-based access control is an approach to restricting system access to authorized users
Router	A router is a device that interconnects two or more computer networks, and selectively interchanges packets of data between them.
SOA	A Service-Oriented Architecture (SOA) is a flexible set of design principles used during the phases of development and integration. A deployed SOA-based architecture will provide a loosely-integrated suite of services that can be used within multiple business domains.
SSL encryption	An SSL encryption establishes a private communication channel enabling encryption of the data during transmission. Encryption scrambles the data, essentially creating an envelope for message privacy.
Storage Area Network	A storage area network (SAN) is an architecture to attach remote computer storage devices (such as disk arrays, tape libraries, and optical jukeboxes) to servers in such a way that the devices appear as locally attached to the operating system.
System Integrity	The state that exists when there is complete assurance that under all conditions an IT system is based on the logical correctness and reliability of the operating system, the logical completeness of the hardware and software that implement the protection mechanisms.
Token	A security token is a physical device that an authorized user of computer services is given to ease authentication.
Universal Serial Bus	Universal Serial Bus (USB) is a specification to establish communication between devices and a host controller (usually personal computers).
Virtual Token	Virtual tokens are a new concept in multi-factor authentication which reduce the costs normally associated with implementation and maintenance of multi-factor solutions by utilizing the user's existing internet device as the "something the user has" factor.
Web Gardening	The scalability on multiprocessor machines can be enhanced by load balancing, each with processor affinity set to its CPU. The technique is called Web gardening, and can dramatically improve the performance

Terms	Description
	of application.
Web Server	A web server is a computer program that delivers (serves) content, such as web pages, using the Hypertext Transfer Protocol (HTTP), over the World Wide Web.
Web Services	Web services are typically application programming interfaces (API) or web APIs that are accessed via Hypertext Transfer Protocol and executed on a remote system hosting the requested services.

1. Executive Summary

1.1 Introduction

Post AS IS study, Requirement gathering activity across all the eight departments under consideration of this project was started. Based on the requirements study and keeping in mind the different functionalities to be expected out of the solution, the next stage was to propose and design a technical platform which would support all such functionalities. The purpose of this document is to provide the design the architecture of the envisaged business analytics solution based on the functional requirements.

1.2 Solution Architecture

Presently various external entities including Insurers are submitting data to IRDA in hardcopy documents or in softcopies sent over email or through the memory disk. There is no central storage of data and reporting system in place so as to generate relevant information out of the raw data in form of reports or analysis. To eliminate the cumbersome and complex manual processes involved in generating information from the raw data, the envisaged solution needs to be designed in such a manner all the different manual processes will be automated and correct information will be available to the business users at right point and with respect to the appropriate context.

The overarching objective of the Business Analytics solution is to provide necessary data and information for analyzing the insurance companies and regulatory decision making.

For designing the solution architecture, the system requirements have been considered as one of the key input. Based on both functional and system requirements different views of the solution has been represented to describe the entire solution in details.

The architecture section includes following components:

- Business Analytics Solution Architecture
  - Reference Architecture - Gives an overview of the entire solution containing the key components of the solution.
  - Functional View - Elaborates various functional components of the envisaged solution. The functional components have been identified based on the functional requirements specified by the business users across departments and across levels during the requirement gathering activities.
  - Overall envisaged technology platform of IRDA system will comprise of a set of applications and services. A number of services will be hosted for internal consumption; typically to manage the business processes and functions of IRDA as an organization and some external services through content, data and application level integration will also be rendered through this platform to the insurer, IRDA customers, employees and management team.
  - The functional view comprises of the following services / applications:

Platform Management Services

- ***Security Services****:* Standard authentication and authorization services, application registration and strong auditing capabilities for the transactions and other pertinent details.
- ***Application Management Services:*** Along with the set of services provided in a typical application server environment, typical IT and SLA management services

Information Dissemination/Rendering Services

- ***IRDA Portal:*** The portal will provide a platform for the extended enterprise to be managed. It will therefore expose both enterprise applications and a number of functional applications to the extended enterprise

Business Applications and Services

- ***Business Applications:*** These will be offered as a platform to IRDA. This platform will be run on the internal environment and will be accessible, to differing extents, through the channels of information dissemination through defined integration touch points.
- ***Internal Applications:*** Hosted enterprise application suite is expected to be in place to manage the internal operations of IRDA in various departments.

Application Design/Integration Services

- ***Services Design and Maintenance Platform:*** Comprises of an integrated development environment providing an interface to maintain services based on the relevant development framework.
- ***Data Integration:*** Data will be resident in multiple repositories of the platform. Some of the data assets might also reside outside the platform in the database of specific application provider e.g. agency portal system

o Information View - This view of the architecture elaborates the flow of information right from its point of acquisition to its point of consumption by the various stakeholders

Following are the layers / components of the Information view through which information passes:

- Data Acquisition Layer
- Data Aggregation and Storage Layer
- Business Access Layer
- Information Delivery Layer
- Information Consumer Layer

o Application View - Elaborates the applications to fit the Functional requirement of the system and to support the Information flow in the system. The application view assumes all the different applications spread across departments would be accessible from the portal using a central integration layer.

- Infrastructure View - Elaborates the Infrastructure need of IRDA to support the applications that has been proposed in the previous view. The infrastructure view comprises of the following components:
  - Central Data Centre (CDC) and Disaster Recovery (DR) site specifications
  - Business Continuity Plan
  - Hardware Infrastructure
  - Network Configuration
  - Scalability Plan
- Security Framework and Architecture - Elaborates the security need of IRDA to safeguard the data, information, other contents, applications from various internal and external security threats. This section describes the different methods, processes and mechanisms such as access control, authentications and encryption mechanisms through advanced solutions like biometric devices and digital signature

2. Objectives of the Business Analytics Solution

The primary objective of the Business Analytics solution is to provide necessary data and information for analyzing the insurance companies and regulatory decision making. Other objectives have been further detailed out below:

- Making data capture simple and timely
- To provide centralized facility to store and process captured data
- Spend less time to capture and maintain data and more time in analyzing the data
- Disseminate Data/ information within Authority for regulatory action – make it effortless and system based
- Providing MIS to various levels of Authority for Administrative and regulatory purpose
- Support evolving need of information/ analysis from various internal and external stakeholders
- Uniformity of data definitions and data format across the departments
- Provide necessary notification on the default/ deviations for non-compliance with regulations

3. Key Business Drivers

The solution has been conceptualized keeping the following business drivers in mind.

- Minimize the complications and time needed to capture data from insurers for the purpose of offsite inspection
- Centralized data storage and share it across the departments within the authority
- Enhanced data analysis capability to support better regulation and monitoring market growth
- Evolving need of information and analysis
- Effective Information dissemination through Enhanced Functionality

4. Solution Themes

Based on the objectives, the following themes are identified for the envisaged solution. These themes are the guiding factors in designing the envisaged solution.

Solution Theme	Description
Single version of truth	A centralized de-duplicated database – all the departments in the Authority will utilize that database to enable cross functional and consistent analysis
Reduced manual intervention	Reduce the time and effort spent both at Insurer end and IRDA end to manage the data
Enhanced Analysis capability	The evolving analysis need of the authority to safeguard the Insured and Insurers and support wholesome growth in the sector
Workflow and Notification	Managing the activities, follow-up action, corrective action etc on time
Transparency	Make information available within IRDA from DD level to the Chairman level without any dependency on individual wish
Information Dissemination	Share and distribute the information to various internal and external stakeholders with role base access control

5. Present IT Infrastructure at IRDA

5.1 Existing applications used in IRDA

Along with the gathering of functional requirements from the different departments, a study regarding the existing IT environment for IRDA was also conducted. The findings of the study were based on the inputs from the IT department and the different documents containing specifications of the existing operational applications used in the organization. The current IT system landscape of IRDA can be divided in to two parts. Web based and non web based systems. Presently IRDA has three websites and the different web based modules/components under each of them are the shown as the following:

- **www.irda.gov.in:**
    - Content Management – Used for storing, controlling, versioning, and publishing industry-specific documentation such as news articles, operators' manuals, technical manuals, sales guides, and marketing brochures
    - Brokers Online Filing – Used for filling up online forms for registering the brokers with IRDA. This facility is available online in this portal.
    - Grievance Management - The grievance management system tracks the new complaint, forwarded complaints, update status of complaints, rending the insurers and generating some customized reports on the basis of the complaints.
    - New Business Statistics – This module is designed to capture new business data for both life and non life department
    - Advertisement - This module is designed to track the details advertisements for each insurer. The module also tracks those advertisements that are released by intermediaries.
    - Third Party Administrator - This module is designed to track the details of the third party administrators
    - Surveyor Licensing System - Surveyor Licensing Module is developed to track the information on the surveyor. It consists of the pre-defined HTML forms which are robust and secure.
- **www.irdaindia.org:**
    - Agency Licensing Portal - This is a system developed for online licensing of the agents and corporate agents
- **www.irdaonline.org:**

Presently there are no components hosted in this website. This website is used for information gathering purpose only.

The non web based solutions at IRDA at present are the following:

- **Receipt and Inward System -** Tracking of inward mails /office notes
- **MIS -** Collecting Regulatory returns from Insurers and Generating Analysis
- **ATI Database -** Capturing new application details of ATIs (both Online / Off-line)

5.2 Existing applications and their status:

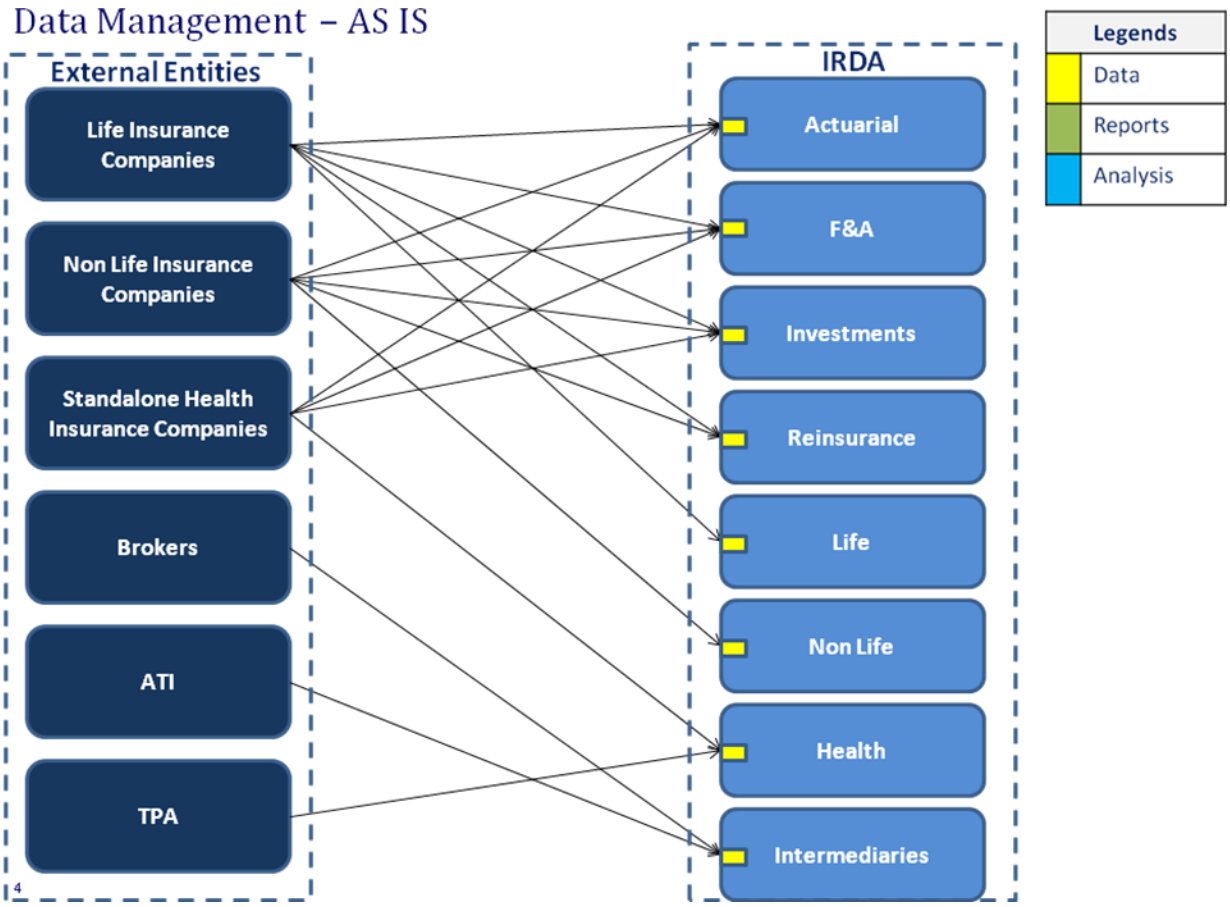
As of now following is the current status of the different applications in terms of usage:

Application	Web Based/ Non-web based	Development Status	Currently used or not	Internet/Intranet/Others
Content Management Module	Web Based (www.irda.gov.in)	Finished	In Place	Internet
Brokers Online Filing	Web Based (www.irda.gov.in)	Finished	In Place	Internet
Grievance Management (Life & Non-Life)	Web Based (www.irda.gov.in)	Finished	In Place	Intranet
New Business Statistics (Life & Non-Life)	Web Based (www.irda.gov.in)	Finished	Currently Not Used	NA
Advertisement	Web Based (www.irda.gov.in)	Finished	Currently Not Used	NA
TPA Online Filing	Web Based (www.irda.gov.in)	Development is not over yet	NA	NA
Online Agent Registration	Web Based(www.irdaonline.org)	Finished	In Place	Internet
eceipt and nward System	Non Web Based	Finished	In Place	Stand Alone Mode
MIS	Non Web Based	Finished	Currently Not in Use	NA

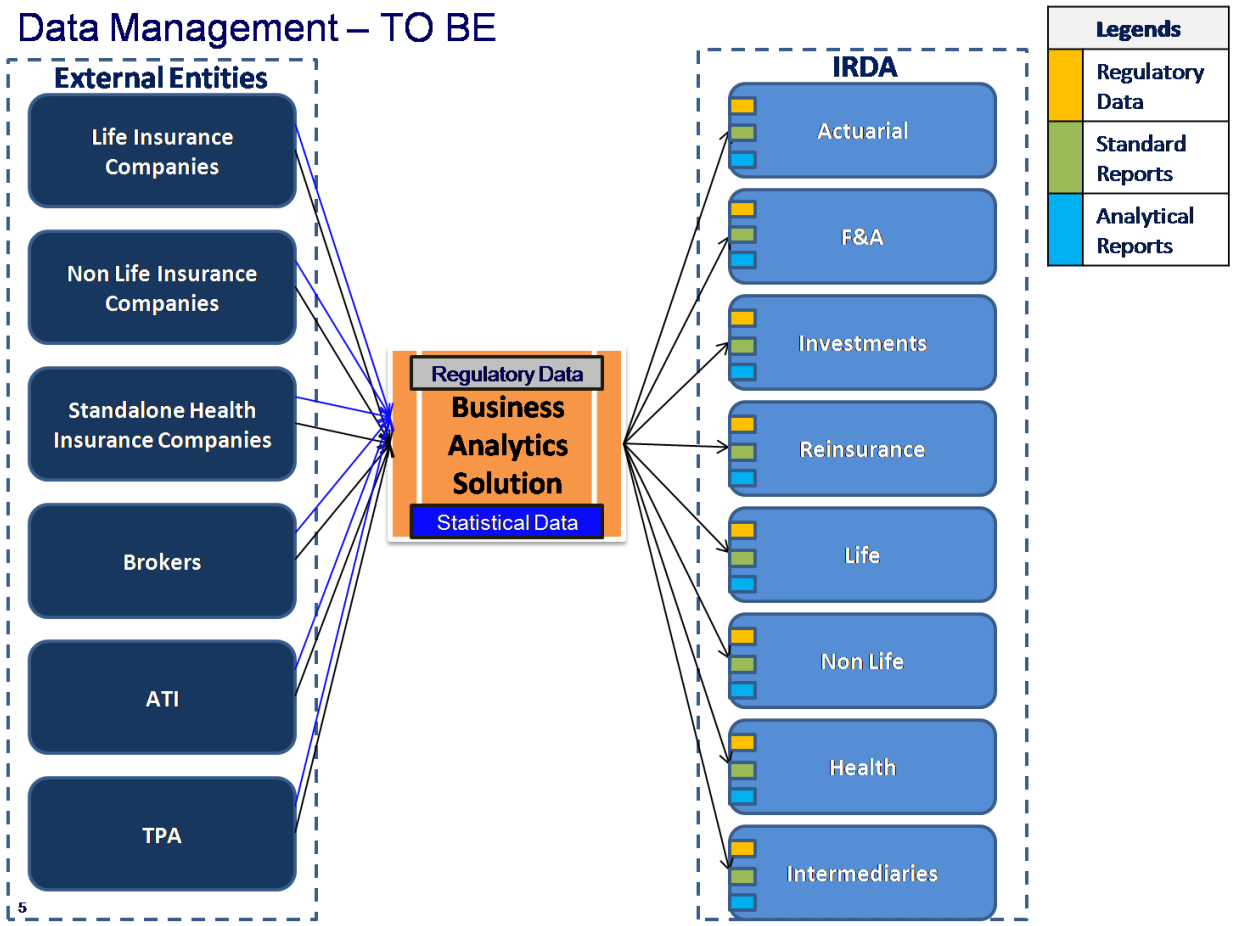
Please refer to the Appendix H of the appendix section for details of all the above mentioned systems gathered from the inputs of the IT department and other supporting documents.

6. Data Management Challenges

Presently different external entities are submitting data to IRDA in form of paper documents and hardcopies. There is no central storage of data and reporting system in place so as to generate relevant information out of the raw data in form of reports or analysis. The process of generating information out of the raw data is highly cumbersome and manual.



In the proposed system, both statistical and regulatory data coming from the external entities will be stored in a centralized data store which will be transformed, cleaned and structured to make them available in form of reports and analysis to both IRDA internal stakeholders and external entities. The diagram below displays the To-Be scenario with respect to data capture and management.


Data Management – TO BE
External Entities
Life Insurance Companies
Non Life Insurance Companies
Standalone Health Insurance Companies
Brokers
ATI
TPA
5
Regulatory Data
Business Analytics Solution
Statistical Data
IRDA
Actuarial
F&A
Investments
Reinsurance
Life
Non Life
Health
Intermediaries
Legends
Regulatory Data
Standard Reports
Analytical Reports

7. Solution Architecture Components

For designing the solution architecture, the system requirement has been considered as one of the key input. These system requirements have been divided into the Functional Requirement and System requirement of the solution. Based on both functional and system requirements different views of the solution has been represented to describe the entire solution in details.

The solution architecture section comprises following components:

- Reference Architecture
- Functional Architecture
- Delivery Channel Architecture (Information View)
- Application Architecture

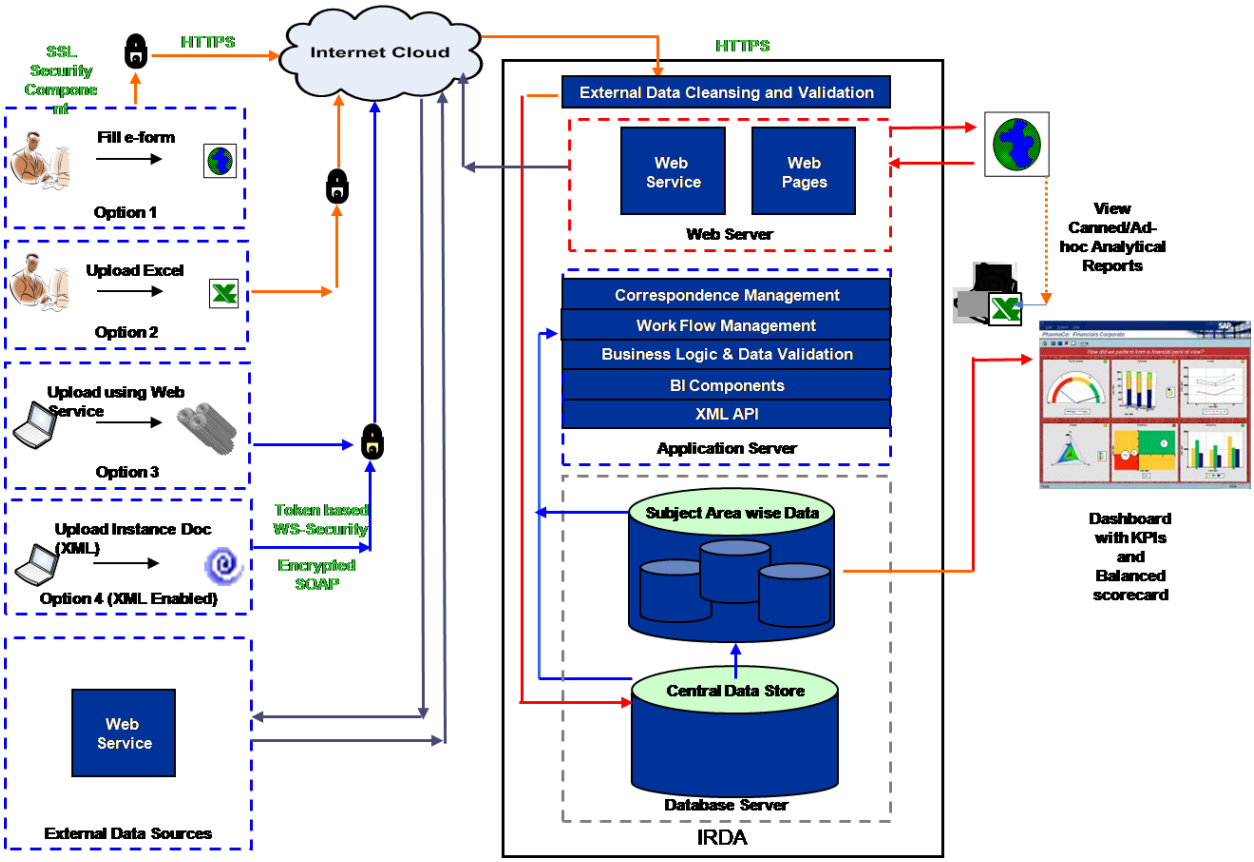
The following subsections elaborate the abovementioned components of the solution architecture.

7.1 Reference Architecture

The reference architecture gives an overview of the entire solution containing the key components of the solution. The Business Analytics Solution has three broad components that interact with each other.

- A front-end portal which acts as a window to all IRDA applications e.g. Insurer data capture and approval.
- A centralized database for having single version of truth
- A view that facilitates regulatory monitoring and understanding of market development activities of the Insurance companies.
- An analytical platform, gathering input from the operational data warehouse, providing analytics and reporting across various dimensions.

The diagram below depicts the key components of the solution.


SSL Security Component
HTTPS
Internet Cloud
HTTPS
Fill e-form
Option 1
Upload Excel
Option 2
Upload using Web Service
Option 3
Upload Instance Doc (XML)
Option 4 (XML Enabled)
Token based WS-Security
Encrypted SOAP
Web Service
External Data Sources
External Data Cleansing and Validation
Web Service
Web Pages
Web Server
Correspondence Management
Work Flow Management
Business Logic & Data Validation
BI Components
XML API
Application Server
Subject Area wise Data
Central Data Store
Database Server
IRDA
View Canned/Ad-hoc Analytical Reports
Dashboard with KPIs and Balanced scorecard

7.2 Functional Architecture

This view of the architecture elaborates various functional components of the envisaged solution. The functional components have been identified based on the functional requirements specified by the business users across departments and across levels during the requirement gathering activities.

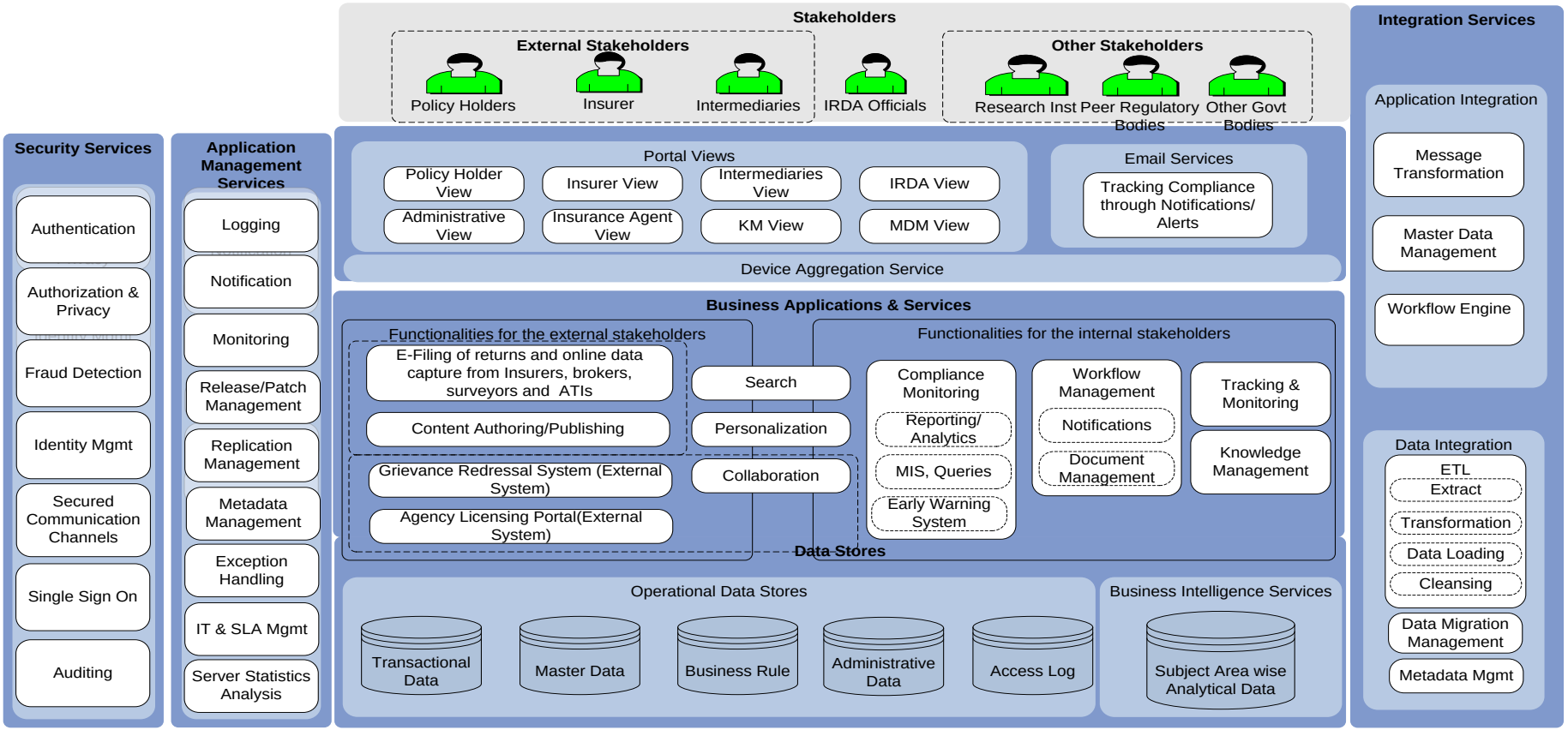
Overall envisaged technology platform of IRDA system will comprise of a set of applications and services that are expected to be rendered through a typical n-tier architecture configuration. A number of services will be hosted for internal consumption; typically to manage the business processes and functions of IRDA as an organization and also it's extended enterprise of estates, vendors and other partners.

A host of external services through content, data and application level integration will also be rendered through this platform to the insurer, IRDA customers, employees and management team. Following sections describe the conceptual view of the overall services platforms

Following diagram depicts the conceptual view of the overall services platforms:

Functional view of the Solution Architecture

The components of the solution architecture, as depicted in the above diagram, will render various services as given in the table below:



Service	Description
Platform Management Services	Platform Management Services comprise of two broad set of service suites- ***Security Services**:* Standard authentication and authorization services, application registration and strong auditing capabilities for the transactions and other pertinent details. A single sign-on process is also expected to be implemented as part of these services that will allow the integration of multiple applications and services through a bound application gateway. Encryption and support for standard encryption algorithm/mechanism like SSL and applicable payment industry standards. ***Application Management Services:*** Along with the set of services provided in a typical application server environment, typical IT and SLA management services in terms of response times and other parameters as well as some application monitoring dashboards are envisaged to be a part of these services. Overall technical architecture and distributed nature of environment is expected to pose some additional integration challenges in this environment.
Information Dissemination/Rendering Services	Content and transactions will be rendered through a number of different channels. Currently, there is only one channel. However, assuming that the number of channels may be extended in future, a device aggregation layer should be planned to make the service delivery device independent. ***IRDA Portal:*** The portal will provide a platform for the extended enterprise to be managed. It will therefore expose both enterprise applications and a number of functional applications to the extended enterprise. The portal should therefore operate through an appropriate parser that is able to render a broad number of services while connected to the portal. Each response request in the portal should be well integrated with the parsing application. The parser application and infrastructure is expected to form a key component of solution design. All the customer- facing services will be available through the portal since it is expected to be the primary gateway for Insurance Companies, Insurance Customers, Peer Regulatory bodies etc. Separate views and instances of applications will be provided through typical portal application. Views should be modularized and customizable to a significant extent. These customizations will be driven by business process and logic.
	Business applications and services may be broadly divided into two categories

Service	Description
Business Applications and Services	***Business Applications*:** These will be offered as a platform to IRDA. This platform will be run on the internal environment and will be accessible, to differing extents, through the channels of information dissemination through defined integration touch points. All the customer facing services will need to have a tightly coupled integration with IRDA service delivery platform. It is critical to capture the data and transaction footprints for these services. Internal applications will also need to have data and application level footprints. Data and application logic will be completely resident on the respective environments. Specific data level integration requirements will be defined during the analysis phase of the project. The applications envisaged are 1. Content Authoring/Publishing Service – A service which allows users to upload/download and access document repositories in the IRDA portal 2. Knowledge Management – The KM portal will contain various documents and information about various activities of IRDA and on the Insurance sector as a whole. This will have two basic sub parts a. Repository of information and documents available to external stakeholders b. Information and documents only available to IRDA employees / users 3. Collaboration Services – Services rendered by the portal however these are not necessarily owned by the portal. Instead these services may e borrowed for other portals or applications 4. Search –Allows users to search for a specific service in the portal, instead of trying navigate to the link for that particular service 5. Personalization – Allows the user to personalize the web pages, look & feel and save favorite links etc. ***Internal Applications*:** Hosted enterprise application suite is expected to be in place to manage the internal operations of IRDA in various departments. Typical areas of operation will be generation of various MIS reports, automated tracking of various compliance deadline (including on time submission of data) for the various companies. All these applications will have tightly coupled integration with the data layer. Internal applications would also include a master data management module to add/delete/modify and manage all key master entities including the hierarchy and roles management. For details of the internal application please refer to business requirements.
Application	This set of services comprises of three categories-

Service	Description
Design/Integration Services	**Services Design and Maintenance Platform** Comprises of an integrated development environment providing an interface to maintain services based on the relevant development framework. The interface will be used to modify and manage the changes in the services description and definition. A typical environment would also contain workflow and rules management engine to provide the ability to design configurable services. **Data Integration** Data will be resident in multiple repositories of the platform. Some of the data assets might also reside outside the platform in the database of specific application provider e.g. agency portal system. A concerted data management strategy will need to be designed. Typical on and offline data integration model should be considered as part of the overall technology solution stack. **Data Stores** Overall application layer will have multiple data stores in two different variations a) Data Stores within the IRDA controlled environment: IRDA will have complete control and direct access to the data being logged/created out of proprietary applications. b) Data Store in Application Providers Environment: Data will be managed by the respective environment owner. While the exact need and a mechanism to pull out this information will be determined during solutioning, there is a currently envisaged need to integrate this data in an online mode. Each application is envisaged to have a dedicated operational data store. From here, an integrated data store providing a 360 degree view of customer and sales information is envisaged as part of this architecture. This data store is expected to receive synchronized and asynchronous feeds from multiple services and applications through an integrated information hub described in the application architecture section.

7.3 List of interfaces for the Business Analytics Solution

Following is the list of interfaces for the business analytics solution. Some of the interfaces are with external solutions. The BAP solution will be loosely integrated with these systems in terms of extraction of data from these systems for reporting and analytics:

External Interfaces:

- IGMS (Proposed Integrated Grievance Redressal Management System)
- Agency Licensing Portal
- Health Database
- Payment Gateway

Internal Interfaces:

- Workflow Application or Business Process Management Systems
- Business Intelligence Application, Analytical , Data warehousing Applications
- Content Management Solution
- IT security Applications
- Intranet
- Data Quality Applications
- Metadata Management Repository

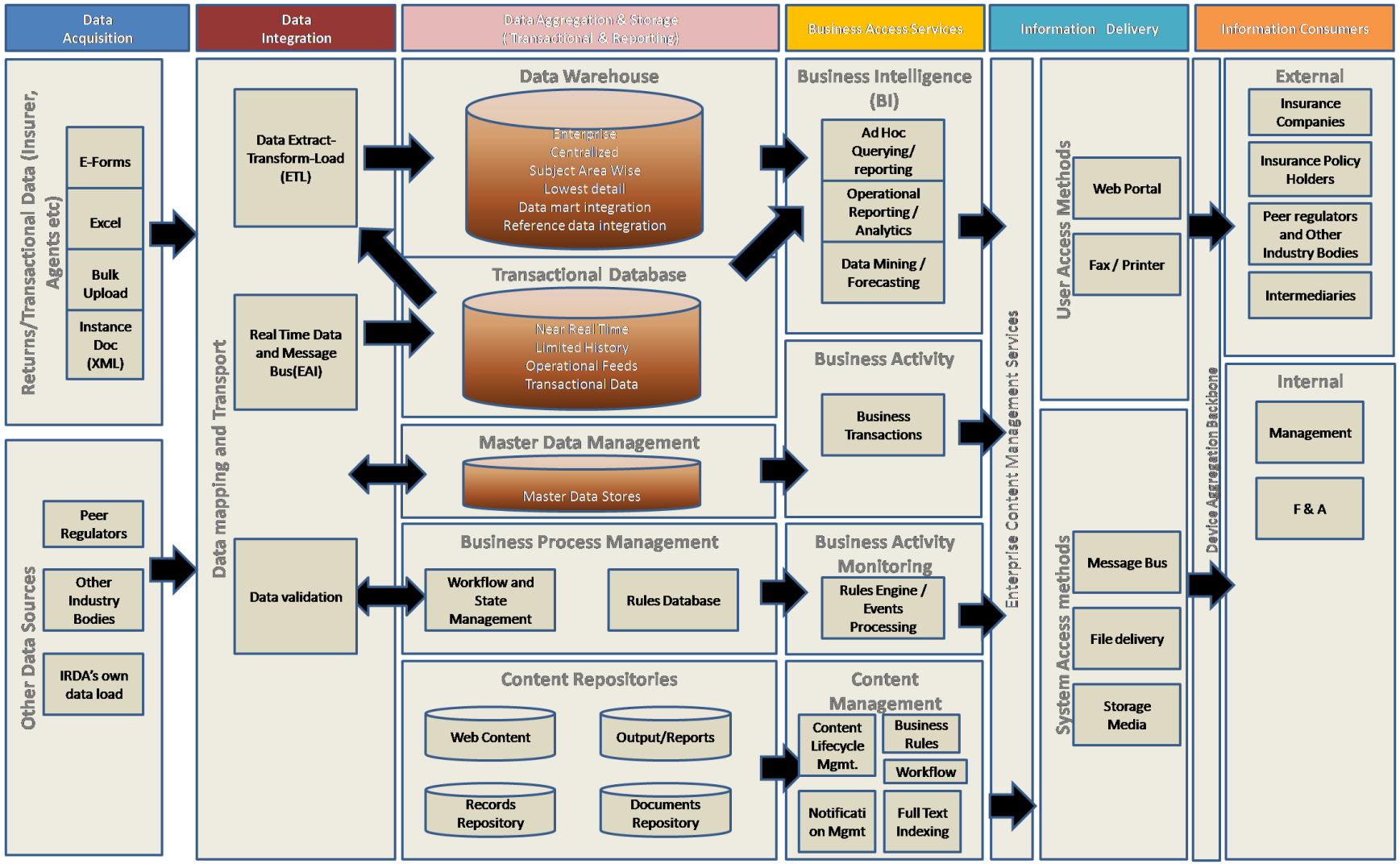
7.4 Delivery Channel Architecture (Information View)

This view of the architecture elaborates the flow of information right from its point of acquisition to its point of consumption by the various stakeholders. The information passes through various layers as following:

- Data Acquisition Layer
- Data Aggregation and Storage Layer
- Business Access Layer
- Information Delivery Layer
- Information Consumer Layer

The diagram in the following page depicts the information flow through various layers:

Information view of the Solution Architecture



The table below elaborates the various layers of the information view and the services it renders.

Information View Layer	Description	Relevance to IRDA
Data Acquisition Layer	This layer is responsible for providing unstructured as well as structured data to the next layer for processing.	
• Operational/Transactional Sources	This is the form of operational data related to day to day transactions, via eForms, Spreadsheet uploads, Bulk Upload etc.	Multiple methods of data acquisition from Insurers
• Reference/Master Sources	This is the reference data which is primarily altered or uploaded by system administrators, and is altered rarely	Master data management on IRDA Database.
• Unstructured Sources	These is the form of data like documents, eMails, Circulars, guidelines etc.	Document management /published by IRDA
Data Integration Layer	For Structured Data: This layer uses data provided by the Data Acquisition layer and processes and transforms the data for use by next layer. It enables data to be used in a more efficient manner as well as makes it more scalable. This layer may also house an ETL (Extraction-Transformation- Loading) program to load the data warehouse. However the most common practice is to load the transactional data in the ODS and use a transformation mechanism like an ETL to move the historical data to the Data Warehouse. For Unstructured Data: This layer has an indexing and Meta Tagging mechanism by means of which the unstructured data is organized.	Data required for various analytical reports for IRDA internal and Peer Regulatory bodies.
Data Aggregation & Storage layer	This layer stores and maintains transformed data received from the Data	

Information View Layer	Description	Relevance to IRDA
	Integration Layer.	
• Data Warehouse	Takes in data from various sources and stores it for reporting and analysis purposes as per the different subject areas.	Data Required for Analytical reporting is stored in the data warehouse
• Operational data store	Handles and stores transactional data.	Primarily transactional data storage i.e. the data as uploaded by insurers
• Master Data Management	Maintain various types of Master Data received from the corresponding source in Data Acquisition Layer.	Master data used in various modules will be centrally administered and maintained from here.
• Business Process Management	Contains the rules database which contains the configurable business rules for managing real time data and transactions. It also manages the workflow which runs across all the applications exposed through the portal. This workflow should be configurable and extendable.	Management of workflow i.e. rules, queues, sequences, authorizations, permissions, notifications etc should be maintained from here.
• Content Repository	Stores and maintains unstructured data like Documents, Web Content, Records, Published reports, etc.	Documents, reports, guidelines published by IRDA
Business Access Layer	This is the layer which is actually responsible for performing business transactional and reporting services. This layer would have some components for	

Information View Layer	Description	Relevance to IRDA
	carrying out business transactions as per some defined business logic (which would reside in Business Activity Monitoring). The business activity services would be residing on top of the ODS and transactional data mart. This layer would also contain the analytical and reporting components such as ad-hoc query, data mining, forecasting etc.	
• Business intelligence	This section is responsible for the various BI and Analytical reports which include Ad-Hoc Reports, Canned Reports, Operational Reports and Forecasting.	
• Business Activity	Primarily defines and responsible for the business transactions.	
• Business Activity Monitoring	This is used for Monitoring real time business transactions and taking necessary actions on defined rule violations.	E.g. Automated email reminders asking for compliance data from insurers.
• Content Management	The takes care of the Content lifecycle management, Workflow provides a feature of full text search and indexing and various library services for the stored content.	Through this layer different documents like company information, research papers etc. will be available to IRDA employees and internal stakeholders.
Information Delivery	This layer enables delivery of various services through the different channels (web portal, email etc.) using various communication methods such as using message bus and through files interchange etc.	

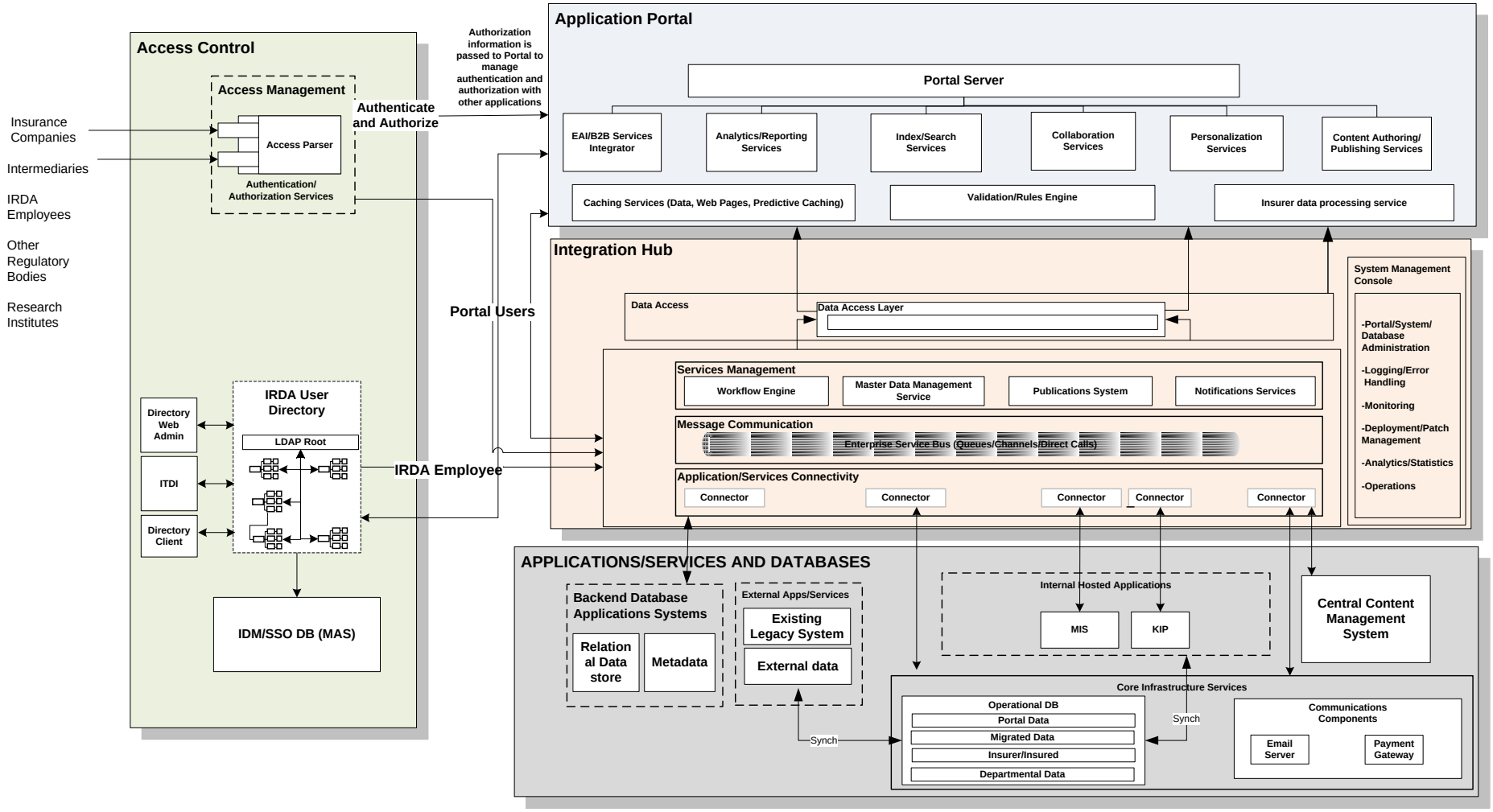
Information View Layer	Description	Relevance to IRDA
Information Consumers	This layer represents the final layer of the information view where the information is actually used by the end users. It enables both external and internal users to use information through reports and applications in place. The external users such as insurers may use the portal to perform some actions for them e.g. upload information to the IRDA portal. Similarly there will be internal users who are employees of IRDA who would be using various applications and reports to carry out their regulatory activities	This layer will be available for viewing reports, performing analysis to different stakeholders like insurers, internal employees etc.

7.5 Application Architecture

This view of the architecture elaborates the applications to fit the Functional requirement of the system and to support the Information flow in the system.

The application view assumes all the different applications spread across departments would be accessible from the portal using a central integration layer. This layer would act as a hub for the overall architecture both from a data and application level communication perspective. This layer will facilitate communication between the portal, different internal applications, back end systems, access management services and all other channels. The diagram below shows a model of the IRDA Business Analytics solution application view.

Application view of the Solution Architecture



IRDA Business Analytics Solution - Application View

Application Components

Following application components are envisaged as main building blocks:

- **Access Management** component serves as a gateway to overall application landscape. It provides for role secured role based access to different views of the portal. This component enables Single Sign-On (SSO) so that users need not sign in again for each of the applications accessed through the portal.
- **Application Portal** components serve as a gateway for all the Business applications, along with content and knowledge management features. There will be different informational/transactional views offered to different stakeholders depending on their role/level of access.
- **Integration Hub** will serve a fulcrum for the overall application view. It will have several components for complex standards-based as well as proprietary integrations, connectivity with all internal hosted application/services, connectors etc. These layers will also serve as on and offline data integration gateway.
- **Application Services and Databases**: Core applications/components that is resident in individual environments as well as hosted infrastructure for IRDA. It includes the Existing data store of IRDA along with the ODS required to run the business applications in Portal.

Each component has been further detailed out below:

Access Management

Access Management component will serve as a gateway for all requests that are routed through web browser. It will use an Employee directory of IRDA along with a SSO/IDM infrastructure to authenticate users. All the external users would be validated against a user credential database. Access Management module should be designed in an open mode with ability to accommodate additional applications and security management solution for new applications.

Application Portal

Application portal will serve as a gateway for requests that may be routed through browser. Portal should be developed using standard portal server. Portal server may have following illustrative components-

- **Knowledge Management Services**: Portal will provide for rich knowledge management capabilities across different departments. A role based view of this system would be given to internal and external stakeholders.
- **Analytics and Reporting Services**: Portal will provide reporting and data analysis features in forms of reports and dashboards.
- **Work Flow Services**: A configurable workflow service would be running across all the business applications.
- **Notifications and Monitoring Services**: A configurable notifications service would be running in association with the work flow service

- **Search Services**: Ability to conduct regular and advanced search.
- **Collaboration Services**: Ability to perform content, data and application based collaboration in line with Web 2.0 principle
- **Personalization Services**: Ability to present customized views (e.g. language based personalization) and modules through a portal depending on the type and nature of users
- **Rules Engine** – Modules to perform basic validation of the data uploaded by the insurers.
- **EAI/B2B Integrator:** Modules to provide data integration services for on and offline data transfers
- **Payment Gateway:** The proposed portal will have an interface with a full-featured payment gateway solution and would provide the ability to process online payments using many payment instruments. Financial Transaction processing component will communicate to the card issuing banks/financial institution through a payment gateway solution. The payment gateway will be invoked from the Integration hub through a request that is raised by the portal. The gateway services will authenticate and process the payment request based on the overall information sent. This payment request status would then be passed back to integration layer and then the results are displayed back to portal.

  The capabilities of the Payment Gateway would be the following –

  Transaction Processing

  - Basic validation of Payment Information
    - MOD 10 validation
    - Well-formed Credit card number validation
    - Card expiry date validation
  - Authentication of payment information
    - Authentication for Issuing Banks
    - Authentication for Internet payment processing
    - Support for services like Verified-by-Visa, MasterCard SecureCode etc
  - Authorization of payment information
  - Capability to ensure atomicity of the transaction
  - Efficient and centralized Reconciliation mechanism

  Security

  - Capability to securely communicate to other third party application/services on the Internet using SSL protocol
  - Protection by Secured firewall
  - Verisign certification

  Administration

  - Checking the status of individual transactions
  - MIS Reports
  - Refunding transactions if applicable

Systems Features

- Industry-standard Scalability
- Industry-standard Performance

Integration Hub

Integration hub will serve three core functions

- Manage the interface between various applications through application to application and application to data integration. Each of the applications may have their dedicated data stores. At a physical level, this may result in separate schema or separate databases. This managed layer will handle the transient and persistent storage of this information.
- Manage the interface between the Business Applications/Services Layer and Presentation Interface: Application/data level integration for internal services and application will be managed by this layer. In addition to managing this interface through a message queue, enterprise service bus, channels or direct RPC calls, this layer will also be responsible for hosting capabilities like workflow engine, master data management components, unified notifications and content publishing services.
- Application/Services level connectivity with the applications/databases that is hosted in IRDA environment will be managed through this integration hub. This layer will ensure loose or tightly coupled connectivity for the different applications.

In addition to these services, a set of common services should also be provisioned for using this integration hub. This would include-

- Content and Information publication management
- Workflow Engine
- Notification Engine
- Master Data Management components
- Business Transaction Services – All the services required to execute the business processes.

Application/Services and Databases

This layer includes:

- Back End systems: These are mostly existing systems with which other business applications need to interact in uni/bidirectional way with respect to information integration.
- Central Content Management System
- Core Infrastructure Services: This would include all operational databases containing data pertaining to different business applications, users, portal metadata etc. It would also include communication components such as Email.

Following are the key considerations for IRDA's envisaged Business Analytics solution:

- **Heterogeneous Environment**: Overall system is expected to have multiple components resident in different and diverse technology platforms. Proper consideration should be given to this point while finalizing the integration architecture.
- **End-to-end Integration (Data Level):** This application would have significant data level integration between legacy systems and the IRDA Portal which will pose a significant challenge in terms of latency, frequency of information. Ensuring the consistency and integration of transaction in a concerted mode will pose a significant challenge to this architecture

8. Architecture Considerations and Constraints

1. The hardware sized for all the applications should be redundant and scalable. All the components within the server should be hot swappable and should incur no downtime due to component failure.

2. All the servers suggested should have dual power supplies. The power input to the power supplies will be from separate Uninterrupted Power Supplies which will be fed from two different power sources. In case of failure of one power supply, the second power supply should be able to take the full load without causing any interruption in services.

3. All servers should have at a minimum of dual 1000 Mbps network interface cards (NIC) installed on different slots. Each NIC will be cabled from a different module on the switch using gigabit speed cabling.

4. The system should be platform independent and should not only be deployable on multiple platforms such as HP UNIX, IBM AIX, IBM i, Sun Solaris, Microsoft Windows, Linux etc., but should also allow integration with other software deployed across heterogeneous operating system platforms.

5. The system should have the capability to use Service Oriented Architecture best practices and should use industry standards for integration to achieve universal use.

6. The system should be database independent and should allow deployment on multiple RDBMS such as DB2, Oracle, and Microsoft etc. The system should allow integration with other heterogeneous databases irrespective of the choice of database for the enterprise system. The database language should be ANSI SQL and should avoid using any Vendor specific proprietary extensions to ANSI SQL (e.g. PL-SQL)

7. Ability to be browser independent. The system should be compatible with the following browsers

    7.1 Internet Explorer 6.0 or higher

    7.2 Mozilla Firefox 3.0.7 or higher

    7.3 Safari, Netscape, etc.

8. The system should have modular structure providing the flexibility to deploy selected modules- products- lines of business combination as per the IRDA's convenience

9. The system should provide fast and steady response times (Quality of Service). The speed and efficiency of the system should not be affected with growing volumes, especially during search operations, data warehousing, reporting, MIS, online processes and batch processes.

10. The system should be operational with good response time using low band width in the region of about 15Kb per user, especially for WAN and internet users.

11. The system should meet the following scalability requirements:

    11.1 Support multi- tier architecture (The Application should at least have the following within its architecture) for all modules within the application with well defined interfaces between the layers

        11.1.1 Presentation Layer

        11.1.2 Business Logic Tier

        11.1.3 Data Tier

    11.2 Capability to integrate with external / third party components like Rules Engine, Functional Modules, General Ledger etc which should not be point to point integration, but with well defined interfaces for data integration using enterprise data model

    11.3 Ability to scale horizontally without redesign

    11.4 Multiple similar hardware and mix of multiple hardware in a horizontal setup.

    11.5 Scalability for external components (External components should not restrict scalability) - Provide performance benchmarks for similar functions required in IRDA for Solution scalability

    11.6 Ability to scale vertically without redesign

    11.7 Addition of CPU, Memory, Hard disk capacity without causing downtime

    11.8 Support the deployment of additional modules at a later point in time with minimal downtime and loss of productivity.

    11.9 Support message patterns and protocols supported - e.g. publish/subscribe, synchronous/asynchronous, push/pull/pool, topics/queues.

9. Interoperability Aspects of Business Analytics Solution

9.1 Challenges of Interoperability

Interoperability is essential for the IRDA business analytics solution. In order to apply Interoperability to the BAP solution the following challenges may arise:

Technical interoperability

Technical Interoperability covers the technical issues of computer systems. It includes also issues on platforms and frameworks. Frameworks for the solution might become complex and many times provide conceptual differences to working approaches. In addition, at times frameworks are duplicative and contradicting with multiple levels. Hence, thorough review and utmost care should be taken while deciding on the frameworks and platforms for the solution. Some of the specific platform and framework related considerations for the business analytics solutions are:

- Choice of the operating system for both client and server
- Option to use server farm and use load balancing to host the portal
- Choice of the browser and it's add on components

Other considerations which are dependent on the platform and frameworks are:

- Portlets built for one portal platform would not interoperate with other portal platforms
- Developers would need to build the same portlet many times to support multiple portal vendors.
- A limited number of portlets will be available from a particular portal vendor for page designers.
- Deployment of portlets may want to be managed on certain systems but "consumed" on other systems.

Organizational interoperability

Organizational interoperability is concerned with organizational processes and cooperation of agencies. Some of the processes may not be enough flexible and adaptive to be integrated and be interoperable. The IRDA top level management will need to play a vital role in such a context. Leadership and strategic direction of management are cited as the most important factors for corporate adoption of Web technology.

Semantic Interoperability

Interoperability or integration efforts are about making information from one system syntactically and semantically accessible to another system. Syntax problems involve format and structure. Semantics being an important technical issue is one that is almost invisible outside technical circles. What it boils down to is that the meaning of apparently identical terms can differ in significant ways between systems. Such differences normally make it more difficult to make systems work together. The

differences can be minimized if systems are designed using agreed data formats. Semantics relate to the understanding and integrity of the information.

9.2 Technology Considerations for Interoperability

There are various technologies that help in achieving the objectives of the business analytics solution by solving the problem of interoperability. Key technologies are discussed below:

Service-oriented Architecture (SOA)

SOA is an architectural style whose goal is to achieve loose coupling among interacting software agents. A service is a unit of work done by a service provider to achieve desired end results for a service consumer.
Service Oriented Environment is based on the following key principals:

- SOA is not just architecture of services seen from a technology perspective, but the policies, practices, and frameworks by which the *right* services are provided and consumed.
- With SOA it is critical to implement processes that ensure that there are at least two different and separate processes—for provider and consumer.
- Rather than leaving developers to discover individual services and put them into context, the Business Service Bus is instead their starting point that guides them to a coherent set that has been assembled for their domain.

.

Web Services (WS)

A web service supports direct interactions with other software agents using XML-based messages exchanged via Internet-based protocols". The Semantic Web infrastructure of ontology services, metadata annotators, reasoning engines and so on will be delivered as Web services. In turn Web services need semantic-driven descriptions for discovery, negotiation and composition.

The encountered problems with development of Web Services are:

- Its ontology building in itself is time consuming.
- The dynamic nature of the field. The exponential rise in the number of bioinformatics Web services over the past year required a further two months effort to maintain and extend the ontology.
- Lack of guidelines on how to build the domain specific ontology, or indeed how to relate it to upper level ontologies.
- Differing interpretation of the myriad of standards – SOAP, WSDL, UDDI, XML Schema etc.; and how they relate

-

10. Conceptual Data Model Design

10.1 Overview

A conceptual data model shows relationships among various data entities to represent high-level dependencies among the data required by business functions/departments. In other words, it shows relationship and interactions among conceptual data entities. It also zooms in on the area of the organization that is the subject of analysis for the project and provides a high-level view representing the business under study for that organization. Entities here refer to the different dimensions / parameters across which different analyses are performed and the facts or measures which are being analyzed across these dimensions. The data model comprises of entities that were defined during the data collection and requirements gathering phases of the project, and includes all entities necessary to support the client's business analytics platform and is developed at a departmental level after analysis of the metrics and reports of the following departments:

1. Life
2. Non – Life
    a. General
    b. Reinsurance
3. Health and TPAs
4. Actuarial
5. Intermediaries[1]
    a. Brokers
    b. Corporate Agents
    c. Surveyors

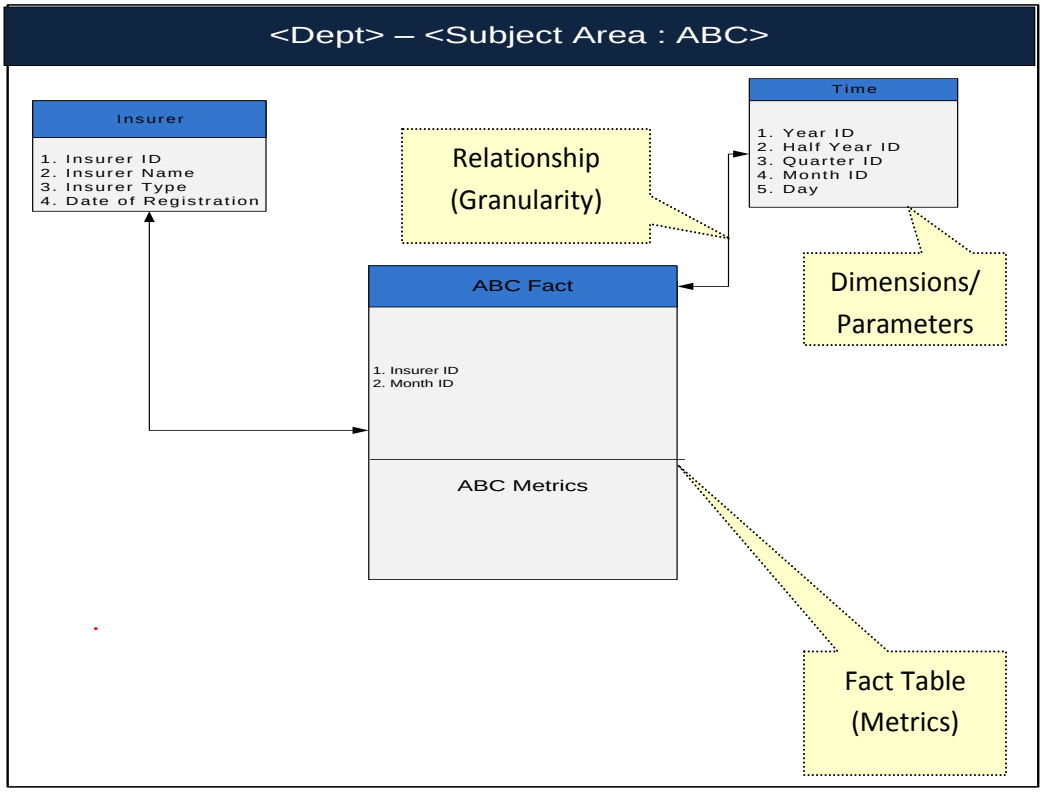
Leaving few forms, owing to the flat dimensional structure for F&A and investment, no dimensional model is suggested for these departments.

Each department is further split into subject areas having similar data elements and analytical context. Similar forms are clubbed together to form a subject area. Each department and the underlying subject areas have a specific set of dimensions or parameters depending upon the analytical requirements. Some of them are common across departments for example time and insurer which are common across

[1] Agents and ATIs data are already captured in agency licensing portal and hence not a part of the dimensional design

departments. Some of them are unique to a particular department such as broker which is relevant only for intermediaries.

Dimensions have attributes in them which are the characteristics metadata elements to further detail out a dimension. A subject area is represented by fact table which represent the metrics or measure in a particular subject area. Dimensions are linked to a fact table using a unique identifier (a key / ID) which shows that the kind of relationship it has with the fact and also the level of granularity at which the metric is analyzed. For example, if month ID is connected with a fact table, it means the metrics in the fact table for that particular subject area are analyzed monthly with respect to the time dimension. It can be represented in the diagram below:



10.2 Form De duplication Matrix

Following the data model, all forms in the particular subject area are listed down along with all the similar forms from other departments. To facilitate the form de duplication process purpose, a matrix have been prepared which shows in a subject area across what dimensions or parameters the different forms are capturing the data. It shows a snapshot of the dimensional commonality across different forms. Also, similar forms from other departments which capture similar data are also shown with their dimensional intersection which helps in finding out the overlaps across interdepartmental data

capturing process. This outcome of this process is summarized and visual snapshot of the commonality of the forms in terms of data capture within and across departments. The structure for this matrix is represented as shown below:

Dept.	Form Name	Dimensions									
		Insurer	Product	LoB	Premium Type	Division	Channel	Geography	Group	Location	Time
ABC	XYZ	X	P				X				M

This represents that form XYZ of ABC department is capturing data across Insurer, product (at the lowest product level granularity) and channel wise. The frequency of the data capture is monthly.

For detailed data models and de duplication matrix for the different departments, please refer to Appendix A.

For the detailed structure of the dimensions please refer to Appendix B in the appendix section.

11. Infrastructure Specifications

This section elaborates the Infrastructure need of IRDA to support the applications that has been proposed in the previous section.

A fully web based application architecture is envisaged that will ensure all the application access is through web. Specific description of different infrastructure solution components along with the rationale is presented in respective sections:

- Central Data Centre (CDC) and Disaster Recovery (DR) site
- Strategy for Disaster Recovery
- Business Continuity Plan
- Hardware Infrastructure
- Network Configuration
- Sizing and Performance Related Considerations
- Scalability Plan

11.1 Data Centre and Disaster Recovery Site

This section will assess the current Disaster Recovery plans, discuss best practices, and provide infrastructure recommendations to meet the recovery requirements of the IRDA Business Analytics Project

Assumptions

The following are assumptions used in developing this assessment:

- This assessment is to focus on the technological aspects of disaster recovery not the business operations
- Current system business continuity plans do not cover the new requirements that will be needed for IRDA infrastructure
- Disaster recovery infrastructure capacity must be able to operate at the same performance level as the primary site
- Does not include overall restoration priority with other systems, such as IGMS.
- Any recommended infrastructure needs are specific to IRDA and thus independent of any other application
- Development environments will be recovered via appropriate backups as time/resource permit upon completion of DR plan execution
- In the event of a disaster, the recovery facility and services should provide the capability to maintain operations of the in-scope the business analytics solution components and related applications for an undetermined amount of time

The proposed Data Centre at can be referred to as the Central Data Center (CDC). Functional and technical resources can be located at CDC and an IT "Help desk" for issue resolution and solution enhancement should be established at the Data Center.

CDC should host various applications, as detailed out in the Application View of the solution architecture.

The Central Data Centre should have full capacity for hosting and running the network/server Infrastructure of IRDA. This should be installed in Hot Stand By mode or back-up in cold state. CDC should act as Primary Data Center and also Business Continuity Planning (BCP) and Disaster Recovery (DR) site for backup of CDC.

In normal situation, CDC should be able to provide services to the different categories of IT users. An automatic load balancer should be installed to divert traffic to least occupied server in CDC. In case of failure of CDC, the DR site should automatically take over the task of failed CDC. DR process should replicate the data from CDC to DR site as online replication. In case of failure of the CDC, this DR should be in a position to take over the entire load automatically.

It is recommended that there should be one "Centralized Data Centres" (CDC) at the IRDA Headquarter in Hyderabad. CDC should be connected to a Disaster Recovery (DR) site and, if possible, established in a different seismic zone, from that of the CDC. Also, if the recovery needs are higher, in such a case, a near site is proposed which will be exactly a replica of the CDC in terms of storage. Further, the computing power of the CDC can be replicated into the near site as well for an almost near real time recovery.

11.2 Strategy for Disaster Recovery (DR)

Disaster Recovery is a strategy used for providing alternate option to at least restore key operations in case problems at main sites. In the context of IT services, typically DR relates to creating backups or having alternate site for restoring the operations. Below is a matrix showing the different types of disaster recovery strategies applicable for the IRDA business analytics project along with their technical specifications:

Recovery Strategy	Technical Specifications
Data Replication	• SAN Replication between the Data Centers for critical data bases needed to meet accelerated RPO requirements (up to 2hours or less of lost data)
Dedicated DB Servers	• Deployment of Recovery Data Center Database Server Capacity to support the critical Data Bases
Dedicated Application Server Capacity for Critical Applications	• Procurement of additional virtualization capacity at the Recovery DC • Purchase of additional applications, middleware, and tool servers at the Recovery DC • CPU, Memory, and Logical Partition upgrades to existing development, test, and stage servers at the Recovery Data Center • Upgrade of the Recovery DC Operations (people and process) capabilities to support production requirements • Expansion of E-mail Infrastructure to support resiliency across the Data Centers
Enhancements to Reduce Recovery Time, Complexity, & Risk	• Wireless Network Deployment • Technology Services Tools Resiliency • BCP Security Access Changes
Tech Services Tools	• Make monitoring and support tools resilient or quickly available at the recovery data center

Technical specifications for the DRC for the IRDA business analytics program

The following with respect to Disaster Recovery is recommended for the IRDA business analytics program:

Technical Considerations

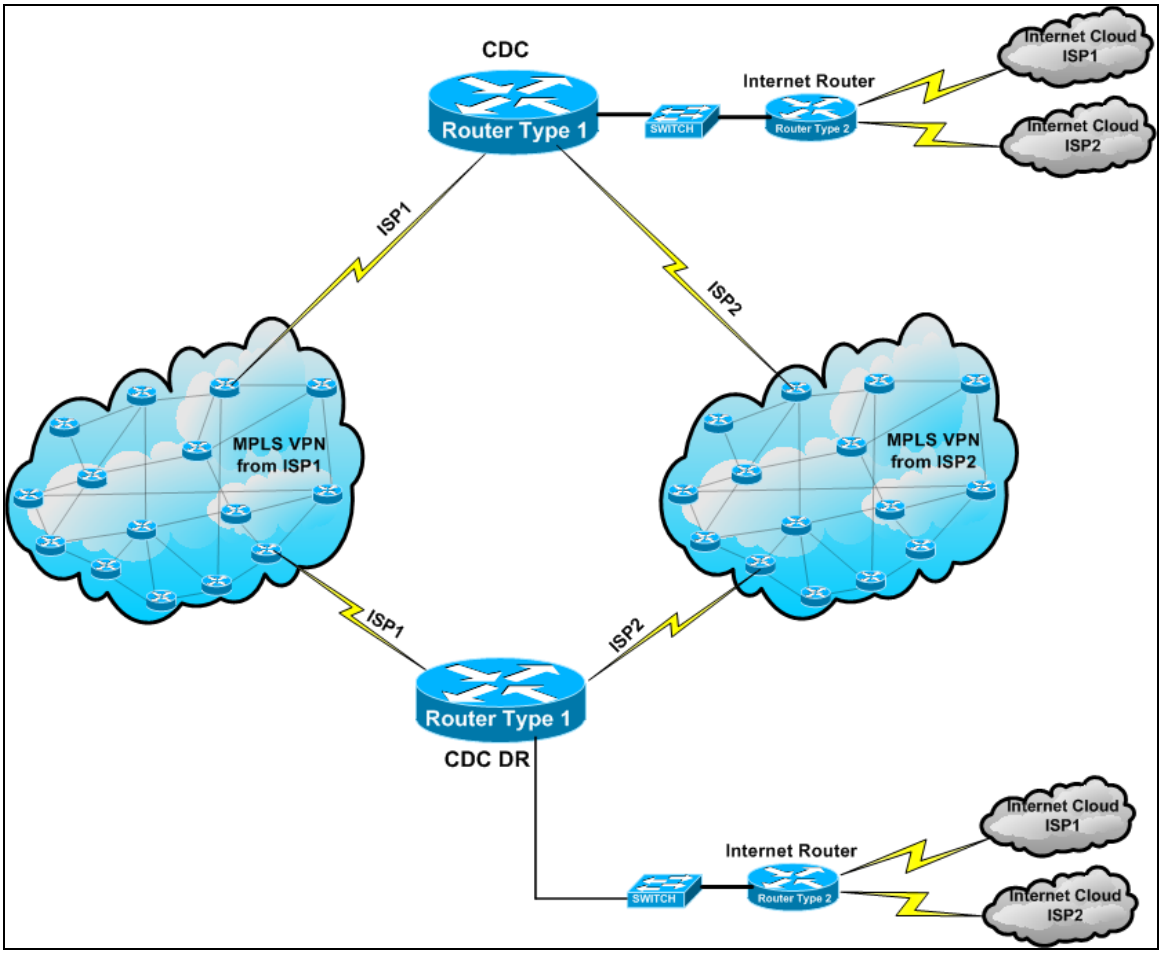
- Network connectivity and sufficient bandwidth will be needed between DC and DRC; burstable bandwidth provisioning should be negotiated with WAN provider(s).
- System software should be used to synchronize platforms at production and recovery locations
- Dedicated equipment is required at the DRC, but it could be used to provide testing or development during normal operations
- Automated provisioning/repurposing of test and development equipment for production/recovery purposes is a recommended capability
- Boot-from-SAN, Ignite or similar process should be used to reduce recovery time
- Regular, full-scale testing of the disaster recovery solution should be performed
- A distinct DR site should be created in the next seismic zone, designed as the backup (mirror) site to the main site. The DR site should deploy the entire application solution (current and latest version of the application builds, and all solution components).

- The DR site should be invoked automatically when the production site fails to provide its services and it should ensure that it supports a degraded performance of at least 80 per cent of that prescribed for the primary site.
- It should be ensured that data is replicated at the DR site at regular intervals
- Routine tests should be simulated to ensure that in case of an emergency, rollover to the DR site happens automatically without any service downtime.
- IRDA should run all services and transactions from the DR Site, at least once in a month, on a non-peak day to check its performance in case of an exigency and service provider (s) should perform DR drills monthly.
- In terms of storage requirements for the DRC, IRDA needs to implement some type of Information Lifecycle Management (ILM) approach. Data needs to be classified and placed on the appropriate class of storage. IRDA needs to implement a synchronous or asynchronous replication approach for critical data (e.g. SRDF, TrueCopy, PPRC, SnapMirror, etc.).
- In addition to IRDA's disaster recovery initiatives, other options also include investigating the use of third party vendors to provide offsite data storage. Offsite data storage services from a third party provider provide a secured means to store critical business and application data in the event of a disaster. Many of these vendors also provide disaster recovery services, which may include the ability to use vendor hardware to run IRDA business applications in the event of a disaster to the IRDA operations center.

Server Side Recommendations for DRC at IRDA

- The servers should be designed in an "Active/Passive" strategy for the SAN replication.
- The servers located in the CDC will continually replicate to the clustered servers in DRC.
- All storage/database servers have matching model numbers, CPU and memory configurations. There are duplicate SAN with identical disk configurations on both sites
- Use of technologies to create and maintain standby databases
- Non-Production servers would be used to support Production during a disaster or extended outage
- As a part of the disaster recovery procedures, all non-production components/servers would be shutdown.
- The production Web and Application servers would be mounted on the non-production hardware from the mirrored copies. The production databases can be started from the standby databases or restored from a backup or mirrored copy depending on the disaster scenario.
- Server Cluster will deliver high-availability functionality to the Business Analytics Solution. This will enable the applications to remain available in the case of a hardware; network or Operating System failure on one of the servers in the cluster group.
- These Server Clusters will be configured with cluster resources required by the BAP application. These resources include network names, IP addresses, application data, services, and disk drives. Once the Cluster resources are brought online it then begins processing client requests.

11.3 Connectivity between CDC and DR Site in normal operation



DR (Disaster Recovery) site should be at a different seismic zone from that of CDC. To ensure undisturbed connection between CDC and DR site the connectivity needs to be at least from two individual ISPs, one is for main network connection and the other is as fall back option. Similarly in DR site, internet connectivity should be same like CDC. It is recommended to have an online replication between CDC and CDC – DR site.

CDC and DR Specifications have been provided in Appendix – D. CDC and DR Specifications.

11.4 Business Continuity Plan

IRDA's Data Centre will host critical applications and database which needs to be protected from various threats of disaster to minimize business interruption/ disruption. Business Continuity Planning is the act of proactively planning a way to prevent, if possible, and manage the consequences of a disaster, limiting it to the extent that a business can afford. Business survival is an issue with all organisations, big or small, due to various threats and vulnerabilities such as:

- catastrophic events - floods, earthquakes, or acts of terrorism
- accidents or disruption by internal or external factors
- outages due to an application error, hardware or network failures

Business survival necessitates planning for every type of business disruption including, but by no means, limited to the above mentioned categories of disasters with results ranging from insured losses of replaceable tangibles to uninsurable capital losses to customer dissatisfaction and possible desertion to complete insolvency.

A business continuity plan is an insurance against such disasters and ensures that key (if not all), business functions continue. A business continuity strategy, then, is a high-value as well as a high-maintenance proposition. In this context, IRDA is no exception and it is as vulnerable as any other enterprise globally.

The key challenge of business continuity preparation is not technology, but the internal "business" aspects that begin at the foundation level of any project and continue throughout its life cycle: such as justification, executive buy-in, broad organizational support, governance and politics.

Perhaps the most important point to make about business continuity support technologies is that its effectiveness depends entirely upon the organization's top-down commitment to the entire project, including updating and testing IT Systems and Infrastructure, recommending suitable policies for maintenance to remain ever geared up for an unexpected turn of events.

Therefore, it is strongly recommended to have a comprehensive Business Continuity Planning and Disaster Recovery initiative at IRDA with full commitment and support from top management and senior executives. Even though Business Continuity Planning (BCP) appears to primarily deal with technology, it is equally associated with the business.

11.5 Recovery Point and Time Objectives for the Business Analytics Solution

The business requirements for IT disaster recovery services were captured by reviewing each of the key business processes within the functional areas of IRDA, identifying for each:

- How quickly following a disaster a particular process needs to be operational (the RTO – Recovery Time Objective)
- The amount of data that can be lost as a result of a disaster (the RPO – Recovery Point Objectives)

In addition, various design attributes relating to the process, such as, if there is a workaround that can be put in place, if it is necessary to be able to perform the process out of the office, were identified.

Functional Areas Reviewed

- Online submission of data and electronic communication management are considered the highest priority functional area for restoration in the event of a disaster.
- Reporting and analytics, tracking and monitoring and workflow are considered to be of medium priority.
- Document and Knowledge Management and other functions like collaborations, search etc. were considered low priority since generally their component processes are not time critical and workarounds are possible providing that the firm can communicate with its clients and access documents.

Business Processes Considered

- Restoration priorities (RTO) align with being able to communicate with the external stakeholders, being able to complete disclosure transactions, and the ability to be able access and update documents.
- Zero data loss (RPO) is required for all the critical functionalities.

Functional Area	Required RTO		
	Between 5 Hours to 24 Hours	Between 2 Hours to 4 Hours	< 2 Hours
Online submission of data			
Electronic Communications			
Reporting and analytics			
Tracking and Monitoring			
Workflow Management			

Functional Area	Required RTO		
	Between 5 Hours to 24 Hours	Between 2 Hours to 4 Hours	< 2 Hours
[2]Document Management			
Knowledge Management			
Support Services and Others			

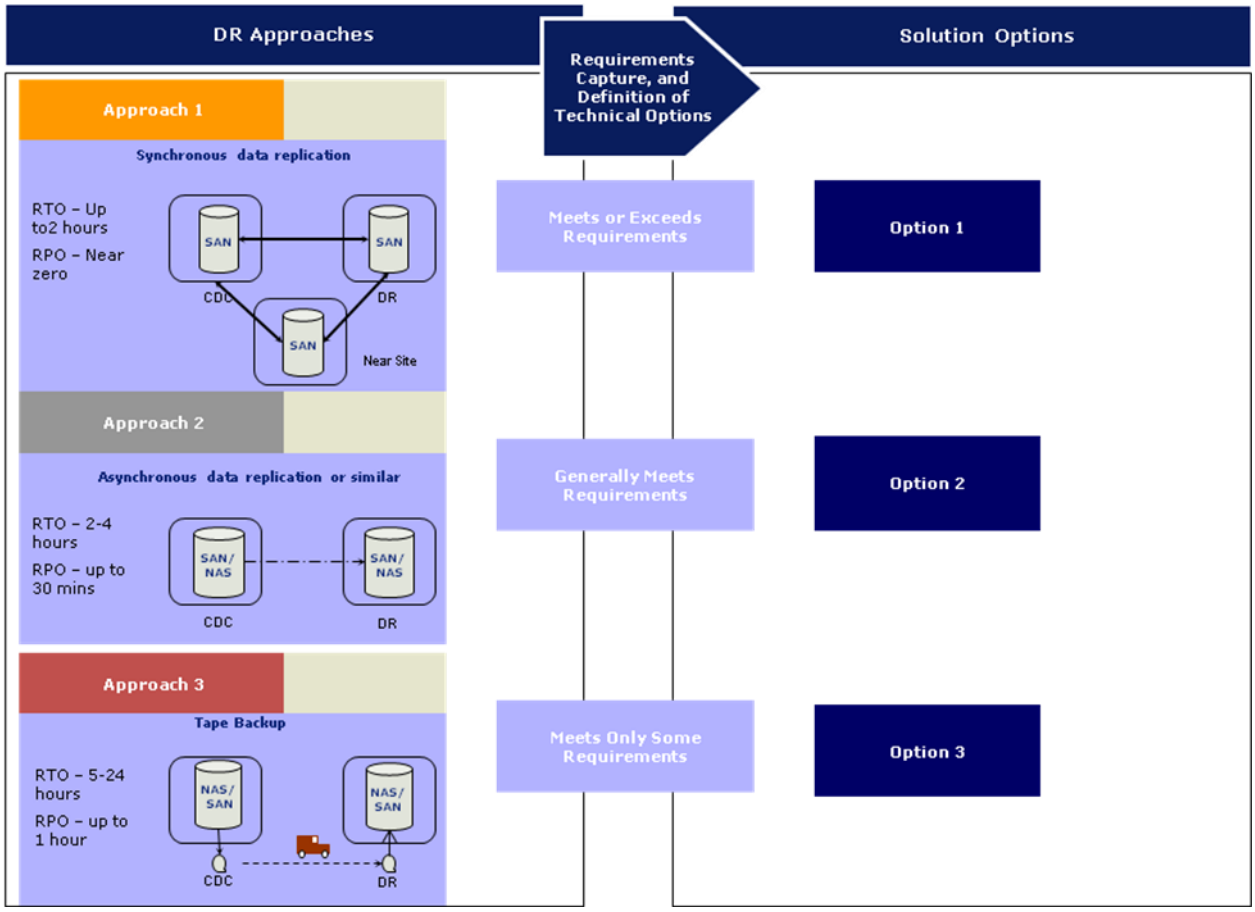
Legends

	Functional Areas with high priority
	Functional Areas with medium priority
	Functional Areas with low priority

[2] Document management can be of medium or high priority at times. The priority of document management can be seasonal at time. Ex. in case of inspection activities or enquiry of an insurer/intermediary.

DR Approaches and Options

- Prior to the capture of business requirements, three approaches to DR were defined providing different levels of recovery capability.
- Following the capture of the business requirements and technology constraints, three solution options were developed broadly in line with the three approaches.

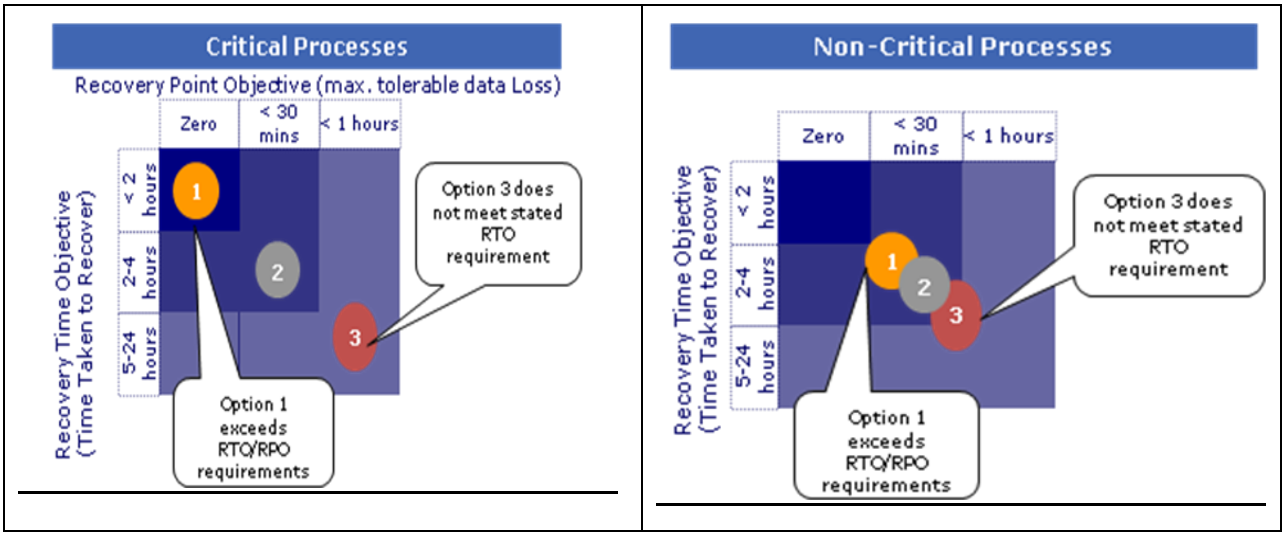


Overview of options and features

	Key Features
Option 1	Data for critical applications replicated in real time between the existing data centre and a near site located outside IRDA. In case of any failures, replication will take place between the DC and near site almost at real time for immediate prevention. In terms of storage capacity and specifications the near site will be a replica of the DC. Depending upon the level of urgency of recovery, the transactional capabilities also can be made available in the DRC. Replication will also take place between the near site and the DRC .Processing equipment in the DR data centre will be maintained for all services. • RPO: Almost zero loss of saved data for critical applications. • RTO: Recovery of critical applications within 2 hours of invocation. • Performance in case of disaster: Same as normal for critical applications, reduced for non critical applications. • Benefits: Meets and exceeds requirements. Simplest failback to production operation requiring relatively minimal outage (e.g. overnight). • Weaknesses: Costs of dark fibres optic links will vary significantly between data centres (careful choice required). Operator error in the near site and the DRC environment could impact production operations. If even computation power is replicated in the near site as well, the costs will go even higher.
Option 2	Architecture similar to Option 1, except that lower performance and cost network links between the data centres are provisioned such that the replication of data between sites will incur a lag. • RPO: 30 minutes of data loss. • RTO: Recovery of critical applications

	Key Features
	within 2-4 hours, although additional testing prior to services coming on line and potential synchronisation errors may cause recovery time to be extended. • Performance in case of disaster: Slightly reduced relative to normal operation for critical applications, reduced for non critical applications. • Benefits: Meets requirements (with some risk on recovery time objective). • Weaknesses: Failback to normal operation requires a planned day of outage.
Option 3	No replication of data, recovery reliant instead on restoration of data from tape. Low priority systems are not maintained, but 'called off' in a DR scenario. • RPO: up to an hour of data loss. • RTO: Recovery of critical applications likely to take 2-4 hours • Performance in case of disaster: Slightly reduced relative to normal operation for critical apps, reduced for non critical apps. • Benefits: DR tests can be handled entirely offline and without interruption to normal operations. • Weaknesses: Failback to normal operation likely to require a planned weekend of outage. DR tests are time consuming.

Options and their fitment to Functional Areas



Options mapping against the recovery requirements

Functional Area	Requirement		Option 1		Option 2		Option 3	
	RTO	RPO	RTO	RTO	RPO	RPO	RTO	RPO
Online submission of data	< 2 Hours	Near Zero						
Electronic Communications	< 2 Hours	Near Zero						
Reporting and analytics	2-4 Hours	< 30 minutes						
Tracking and Monitoring	2-4 Hours	< 30 minutes						
Workflow Management	2-4 Hours	< 30 minutes						
Document Management	< 7 days	< 2 Hours						
Knowledge Management	< 7 days	< 2 Hours						
Support Services and Others	< 7 days	< 2 Hours						

Legends	Description
	Expected to meet requirement

	Higher operational risk in meeting requirements
	Does not meet requirement

Comparison of Options

- Option 3 provides some improvements over the current state, primarily the certainty that a facility and systems will be available to recover the services. However the RTO objectives for priory areas would be not met and recovery relies on relatively unreliable tapes. Option 3 is not a recommended approach given the scale of incremental investment required relative to the benefit delivered.
- Option 2 meets most of the business recovery requirements and will cost lesser to implement than Option 1. However, the cost difference is not as large as anticipated because the asynchronous replication software costs more than the synchronous equivalent and is licensed by terabyte of data replicated. This is likely to result in recurring charges increasing more sharply in this option, than in Option 1 (where the software is licensed per device).
- Option 1 meets the business recovery requirements. Assessing these options against selection criteria including IT operational risk, cost and match to business recovery requirements, Option 1 can be the preferred solution. The relatively small incremental costs brings:
    - minimised data loss (zero for saved data in critical processes),
    - faster recovery of services,
    - relative ease of failback, negating any prolonged period of outage,
    - ease of maintainability and
    - a potential platform for further improving continuity in the future through ‘stretching’ primary services between the DC and DR data centre. Although this would be at extra cost, it is not possible with other options.

11.6 Strategy for Business Continuity Planning (BCP)

In the context of IT services, typically BCP relates to creating backups or having alternate mechanism for providing un-interrupted continuous services during a crisis. Adherence to the following list ensures that the BCP strategy works with utmost ease at the time of any contingency.

- The Alternate Site (AS) should be exactly like Main Site (MS) in storage capacity and should share standby for each other in case of failure, switching immediately in case of a failure. The performance level should not go below 80% in case of failure of either site.
- During normal operations, both main site and alternate site should be running in the "Active-Passive" mode with an automatic load balancer between them, sharing 80 per cent of the full envisaged load.
- Maximum time for a down site to recover should be 24 hours.
- Minimal data loss should be envisaged during failure and that too only to the extent of data being in the transmission lines. Also, all such incidents should be suitably notified to the clients/users.
- A drill should be carried out randomly once every month to test the BCP functionality.
- Vendors should be encouraged to suggest their own business continuity plan during tendering process. Evaluation of solution proposed by the vendors and SLAs proposed by them should be key parameters for evaluating the technical proposals.

BCP (Business Continuity Planning) addresses the following types of failure

LEVEL 0	
Failure	**Solution**
Failure of a component in a machine (Machine can be Network Infrastructure Devices and Servers and High-end user's Systems)	• Each machine should have 100 per cent fault tolerance capability. Fault Tolerance feature should be restored immediately • The faulty component should be replaced with a new component and it should be sent for repair/warranty replacement, etc at the earliest.
LEVEL 1	
Failure	**Solution**
Failure where the machine comes to a halt (Machine refer to Network Infrastructure Devices and Servers and High-end user's	• Each machine should have a backup counterpart. • During problem/breakdown of a machine, backup machine should automatically take over the job of primary machine • The faulty machine should be replaced with the new machine, which should be sent for repair/warranty replacement etc.

Systems)	
LEVEL 2	
Failure	**Solution**
Failure which causes the complete site to halt	• Two similar sites (one CDC and one DR site) have been proposed which should always be up and running for normal operation. In case of higher recovery normal expectations a near site is also proposed which will get replicated at almost at a near real time. • In case of problem/breakdown of a site, DRC should automatically take over the entire load and should start functioning as the primary site. • The status of faulty site shall be restored to normal as soon as possible.
LEVEL 3	
Failure	**Solution**
Failure which causes the entire site to halt, including DR site	• Options such as hiring data center services from ISP vendors, etc. should be explored and latest backup should be restored to start the operation. • Efforts should be made to restore the normal status of main sites and DR sites at the earliest

12. Service Level Agreement for IRDA Business Analytics Solution

This section broadly outlines the various services to be carried out for the business analytics project

12.1 Description and Scope of Services Covered

Services	Description
Development and Implementation	This service delivers the development and delivery of the application as per functional requirements specifications and technical specifications
Training	This service captures end user training and system administrator training.
Application Support	This service captures bug fixing, fixing problems in the application and responding to calls with respect to the application
Service Monitoring	This service captures events (IT alarms, alerts and notifications) in the IT infrastructure and forwards them to appropriate personnel or systems for further action.
Identity/Access Management for Infrastructure.	This service manages and administers access to systems and services in the infrastructure through user IDs, passwords and access control lists.
Problem Management Support	This service proactively reduces incident occurrences by identifying their root causes and takes actions to coordinate development of workarounds for Known Errors and actions to remove those errors from the application
Incident Management Support	This service coordinates actions to restore normal business operations as quickly as possible and minimizes the adverse impact on business operations when agreed service levels are threatened.
Backup/Restore Management	This service provides backup and restoration of data, applications and systems used to underpin IT and IT Business Support services.

Services	Description
Release and Deployment Support	This service plans, manages and coordinates activities to deploy service solutions as set out in release packages.
Configuration Management Support	This service provides identification, tracking and control information about service configurations in an accurate manner and makes that information available to all infrastructure services.
Service Testing	This service ensures that new or changed IT services and their supporting infrastructure are adequately tested and accepted for successful delivery and operation.
Production Assurance	This service provides oversight and testing of new services and service changes prior to them going to production operations.
Knowledge Management	This service manages and administers knowledge repositories, subscriptions and information to ensure that the right information is delivered to the appropriate place or person at the right time.
Capacity Management	This service ensures that all current and future capacity and performance aspects of the application are provided to meet business and service requirements at acceptable cost.
Availability Management	This service optimizes the capability of the services and supporting organization to deliver sustained levels of service availability that meet business requirements at acceptable costs.
Solution Design Services	This service plans, and designs solutions to support business services, processes or functions.
Storage Management	Provides a service to maintain and support infrastructure digital storage assets used to underpin IT and business services.

13. Sizing and Performance Considerations for IRDA Business Analytics Program

This section illustrates the methodologies to be followed and considered for data and hardware (server) sizing for the data storage for IRDA business analytics project. The exact calculations can be performed during the design stage when all the table structures will be designed and ready to be developed.

Data Sizing

Sizing of the database exclusive of the indexes

The template below will capture the sizing estimates for the databases excluding indexes.

Database Name	Table Type (Fact/ Master /Others)	Table Name	Length of the Row (B)	Number of Rows(C)	Estimated Size (D=B*C)	Total (E=D* No. of Years of History Data)
Total						

Inputs Required:

- **No. of Rows:** For master tables, the no. of the members in that particular dimension along with their attributes will be the measure for the no. of rows in the particular table. For fact table it will be the combination of all the members in different master tables together. For example, if there are 3 master tables, M-1, M-2 and M-3 having 3,4,5 members respectively, the total rows in the fact table will be 3X4X5 = 60 rows. For the other transactional tables, an empirical or estimated no. of rows can be captured which is typically a percentage of the total no. of rows in the fact table.
- **Row Length:** The data type represents the length of a row or the data storage for a particular row. If the data type is VarChar it will be 8kb and if it is a SmallInt it will be 32 KB and so on. The number when multiplied by the no. of rows will give the estimate for the data size for the entire

table of a data base. This estimated number when multiplied by no. of years of history data will represent the total storage size in KB.

- **No. of Years of History Data:** This will be typically the years of history data needed to capture for tracking, monitoring, reporting and archiving.

Sizing of the database inclusive of the indexes

The template below captures the sizing estimates for the databases including indexes. This is the minimum real memory requirement for the different database tables.

DB Name	DB Size (KB)	Indexes (KB)	Total (KB)	Total (GB)
Total				

Inputs Required

- DB Size (From previous calculation)
- Index Size

Sizing of the database for incremental increase in data on a year on year basis

The template below captures the server for the data stored in the data bases based on incremental growth of the data on a year on year basis. The incremental increase in data needs to be estimated for this case.

Scenario	Total Size (KB)	Incremental Rate (%)	Total Size	Data Rate (KB/sec)
Indexed				
Not Indexed				

Inputs Required

- Total Size of the databases (From the previous calculations)

- Estimated incremental Rate of Increase in data (on a YoY basis)

Load Estimation

Estimated Query Response Time

Theoretical calculations can be carried out on the queries to estimate the load on the network connections. The usage assumptions (given below) can be used to complete this analysis. Also, data from sizing estimates of the data stored can be used in calculating the average length of rows and the total number of rows

The theoretical estimated query response is captured in the table shown below:

Load Volume	User Types	Max Rows	Bytes/ Row	# Times User's Access System/ Second	Number of Concurrent Users	GB / sec
Scenario A: Maximum Load	Light Users					
	Medium Users					
	Heavy Users					
Minimum Response Time (in secs)						
Scenario B: Typical Load	Light Users					
	Medium Users					
	Heavy Users					
Minimum Response Time (in secs)						

Inputs Required

User profiles and assumptions

The following assumptions associated with corporate query workload are defined in estimating the required computing resources for the IRDA BAP solution data storage:

- Light users create approximately 1,000 bytes each transaction, with 15 transactions an hour for an 8-hour business day
- Medium analytical processing/relational online analytical processing (OLAP/ROLAP) users create approximately 4,000 bytes each transaction, with 20 transactions an hour for an 8-hour business day
- Heavy create approximately 75,000 bytes each transaction with 10 transactions an hour for an 8-hour business day

Based on the above assumptions, complete the workload assumptions below:

Workload Inputs

The following assumptions associated with corporate user demographics are defined to assist in computing resources required for the data storage for IRDA business analytics:

- _____% is heavy-users conducting exhaustive analysis with query tools supporting multidimensional analysis
- _____% of the medium user community is medium users requiring online analytical processing of large volumes of data
- _____% perform simple to medium complexity queries against the data warehouse

Applications Specifications

Application specifications will enable determining data load to and from the BAP solution with respect to the queries in question:

The following factors need to be considered when setting the requirements:

- Complicated Calculations
- Number of Users
- Hardware Specifications
- Data Size

The template below can be used to capture definitions of simple, medium and complex queries:

	Measures	Dimensions	Time Period of Data (In Years)	# of Table Joins	"Group By" Statements

Simple					
Medium					
Complex					

From the template above, the application usage for the different applications can be found out:

Application Name	Query Complexity (Simple, Med, etc.)	Frequency	# of Concurrent Users	Data Transfer Rate (KB/Second)

The no. of users' information can be found out from the users having access to the different applications.

Network Sizing

The purpose of this section is to determine the network (LAN/WAN) usage requirements and identify the loads that may be placed on the network by the system.

The assumptions and inputs required to perform network sizing for the IRDA Business Analytics solution are:

- Volume of data requested by a user query
- No. of queries generated in a particular time span by concurrent users
- The highest volume of data for any of the queries shouldn't exceed beyond a certain threshold
- The row of a database will have a defined average size
- A maximum of X concurrent users will execute the queries at a time.

These assumptions/inputs will be captured for both the scenarios of maximum load and normal load.

Data from this analysis can be captured in the template shown below:

Load Volume	Rows/Month	Bytes/ Row	# Times User's Access System/ Second	Number of Concurrent Users	Kilobytes / Second
Scenario A: Maximum Load					
Scenario B: Typical Load					

From the template above, describe the network usage between the different servers:

Applications	Rows/Month	Bytes/ Row	System Access/Second	# of Concurrent Users	KB/Second

For detailed data sizing of IRDA BAP for the different departments, please refer to Appendix C

14. Scalability and Obsolescence Plan

As the IRDA portal envisages a potential user base of insurers, employees/management of IRDA, Scalability is must-have aspect to be incorporated in the solution architecture, design, implementation and management. The proposed solution tries to meet the scalability requirements from a number of angles, such as:

Technical Angle

The following components of the technical solution would help cater to the envisaged scalability requirements. These have also been covered in the application architecture section.

- Load balancing – this component would provide load balancing capabilities for incoming requests, thereby allowing the portal user traffic to be uniformly serviced by a number of front-end servers. Application Server Web Caching would be used for providing this functionality.
- Caching – Caching services would provide a universal view of the caching by means of caching of the following
    - Web content
    - Data
    - User Information

  This would be made possible by retaining versions of rendered web pages, common web page areas (headers, footer and navigation panels), frequently accessed data, rarely changing data from external applications/services. Caching would result in greater performance, responsiveness and scalability by reducing repeated database access for same data, execution of web page generation logic, cross-system calls or business logic. Caching layer would have built-in intelligence to hold data in the memory based on frequency of access, change frequency, user behaviour. Techniques to invalidate the cache when newer data is available would also be applied.
- Database – The database design, development and operational plans would be designed using proven best practices for data centric applications to ensure maximum possible scalability.

Operations Angle

From an Operations perspective, the following best practices would be followed to ensure scalability.

- Regular database re indexing
- Well-defined database maintenance plans
- Well-defined maintenance plans for servers
- Diagnostic tuning of servers to ensure best performance
- Quick Failure Isolation and replacement of faulty components

- Periodically measure the system performance counters of the server using System Management Console to ensure that the hardware is scaling up
- Disable unnecessary heavy performance logging in the system. (e.g. Windows PerfMon)
- Defragment the storage periodically
- Check the storage health periodically

Infrastructure Angle

From an Infrastructure perspective, the following best practices would be followed to ensure scalability.

- High Availability: Application, Web and database servers need to be designed in failover and firm mode with an ability to ensure full-proof operations
- Redundancy: Adequate processing and capacity redundancy need to be built in within the system to ensure zero to minimal disruption in the overall operations
- Optimal network design to ensure best bandwidth usages
- Consider the use of Web Gardening
- Ideal recycle times for the Web Server process. Ensure that it is set to be recycled based on the resource utilization.

15. Security Framework for IRDA Business Analytics Solution

15.1 Application Security Strategy

The strategy for IRDA Business Analytics application level security including all development production instances is to grant security access on a "least privileged" basis. The least privileged security approach will restrict users only to the components and reports that they require access to, in order to perform their job. This will be accomplished by implementing an "All Doors Closed" approach to application security within the Business Analytics Solution. This means that by default, users will be prevented from accessing interactive applications and data unless they have been explicitly authorized. Security levels and techniques will be applied within the solution to achieve this objective, balancing security requirements with business needs.

This security strategy will be implemented in a manner that provides for as efficient administrative process, as possible after go live.

Basic application security will be used to prevent access to key configuration and administrative applications. Action, processing option and other security methods will be implemented to further secure allowed objects.

Access to applications, reports, and tools will be granted on an individual role basis. Each user will belong to a security role to which security will be applied. IT will be allowed for the users to belong to more than one security role. In general, the security roles will be designed such that each user will only have one security role per environment. Security will be applied at the Role level, not the user level.

15.2 Security Considerations

IRDA will be utilizing many environments within one instance of the Business Analytics Solution during the design and implementation process, through to production. Users can be assigned specific environments and secured out of the remaining environments depending on their involvement in the development and testing of the system design. Each of the environments will have its own set of business data. Data in one environment cannot be accessed unless specific access is granted to a User or Role to that environment.

It is recommended that an audit of the user list be reviewed periodically after go live, to help to ensure that users have been assigned appropriate environments and to identify unauthorized access to the Production environment.

Environment	Environment Description	Purpose
PD	Production	Live System
TR	Training	Training of Users
QA	Quality Assurance	Validated Testing
DV	Development	Development Environment

The following table shows a list of access by environment for the development and project teams as well as end users.

	PD	TR	QA	DV	CV
Key Users	N	N	Y	N	N
Administrators	Y	Y	Y	Y	Y
Project Team	N	N	N	Y	Y
Training	N	Y	N	N	N
Production Support	Y	N	N	N	N

15.3 Approach for Security Types

The following is the strategy for utilizing the security options for the IRDA Business Analytics Solution

1. ***Application Level Security*** plays an important role in the security strategy and approach for mitigating risks in the "to be" environment after go live. Application security will be used to block all users leaving the administrators to run and install components on the top of the solution. This will in effect restrict users from running application or batch objects, by default.

2. ***Action Level Security***

   To simplify security configuration the following variations of action security will be configured:

Setting	Change	Add	Copy	Delete	Scroll
VIEW ONLY	N	N	N	N	N
CHANGE ONLY	Y	N	N	N	N
ADD ONLY	N	Y	Y	N	N
NO DELETE	Y	Y	Y	N	N
FULL ACCESS	Y	Y	Y	Y	N

In interactive applications with drill down options, the security options must also be configured for that user or role to be able to drill down.

3. ***Row Security*** will be used to restrict access, through Business Analytics Solution, to the data in tables. The use of row security will be limited to situations where the other security types prove to be insufficient, due to the system performance implications.

4. ***Column Security*** will be used to restrict access to the data in the Business Analytics Solution data tables and in applications and forms. As this security type does not have any significant impact on performance, it is expected that this security will be used in the IRDA BAP security design, in compliance with business requirements, in order to protect key data fields.

5. ***Form Security*** will be used to restrict end users from opening unauthorized and restricted data input forms for data entry.

6. ***Report Security*** will be used to restrict access, through Business Analytics Solution, to the unauthorized static and canned reports.

7. ***Analytical Security*** will be used to allow end users access to searching/selecting tables or business views (i.e., creating ad-hoc queries).

8. ***Design Security*** will be used on a need-only basis in the IRDA security design. This security restricts or allows the role the ability to make changes to the web pages/tabs/forms/reports/RDBMS and other components within the entire solution. Here typically the access will be given to System Administrators.

15.4 Other Security Considerations

1. ***Version Level Security***
   Version security is enabled for an application only if access to its version has to be restricted from appearing on menu of a particular role(s). If application security is applied to an object, then it includes all versions by default unless it is specifically denied. If application security is applied to a specific version, it will take precedence over security applied to the general object.

2. ***Roles & Environment***
   Environments are defined at the Role level. A role needs to be explicitly granted access to an environment before privileges assigned to the role can be effective in that environment

15.5 Role Based Security Strategy

Security roles will be based on the functional business process designs to be created by the business analytics implementation team and will be approved by the business process owners. Users will be assigned to these roles by the IRDA's business process owners based on the user's job functions.

IRDA will develop separate user roles for the following groups of users:

- Technical and Power User type roles
- End User Functional Roles
- Data input Roles (Roles designed specifically for the external stakeholders such as insurers and intermediaries etc.)

For the detailed security setting for the IRDA business analytics project, please refer to Appendix F

15.6 Technical Framework for Security

This section elaborates the security need of IRDA to safeguard the data, information, other contents, applications from various internal and external security threats. a three tier security system is proposed for the Business Analytics Solution, as following:

- Application
- System and
- Network

The abovementioned security tiers will cover the various security aspects as following:

	System & Information Integrity	Identification & Authentication	Access Control	Audit & Accountability	System & Communication Protection
Application		Multi Factor Authentication Digital Signature	Role Based Access	Audit Logging	SSL Encryption
System	Software Integrity	Strong Passwords Identity Management	Role Based Access	Audit Logging	Firewall HIDS/NIDS
Network	Multi Factor Authentication	ACLS	Audit Logging	Multi Factor Authentication	ACLS

Each security tier has been explained in details the Appendix E

16. Data and Document Migration Strategy

16.1 Data Migration Objectives

The key data migration objectives of the Business Analytics projects are to:

- Migrate active transactional data from source systems to target solution with no deterioration in data quality;
- Provide read only access to inactive transactional data either through solution or alternate reporting mechanisms; and
- Dispose of any redundant data.

There may also be a requirement for migration routines to be developed to populate reference data within the new application or sub modules.

16.2 Data Migration Scope

Data Sources

The data sources that needs to be considered in data migration activities are

- Hardcopies
- Excel Spreadsheets
- Text Files
- MS – Word Documents
- Existing legacy systems databases

16.3 Data Migration – Business Considerations

The historic data that is not required to be migrated into the new application will be retained offline.

Ideally the Regulatory Programme data migration approach would adhere to the business' archiving strategies and standards and utilise existing archiving approaches and solutions. From a migration perspective three options are available as a stop gap arrangement in case of absence of a formal archiving strategy:

	Option	Pros	Cons
1	Migrate all 'Active' and 'Inactive' data that the business cares about into the new applications. Once the archiving solution has been developed for the new application the migrated data can be archived via the solution as per the business archiving strategy.	Consistent archiving approach can be taken. Logic for migration datasets may be simplified. Users have access to live and historic data through the same interface.	Large volumes of data that is not required within operational systems which may impair performance and usability of new application functionality. Development of archiving strategy and solution may be some time after new applications are implemented.
2	Data requiring offline access is migrated to an enterprise reporting / warehouse solution.	Enterprise warehousing solution could provide ability for the business to conduct ad-hoc reporting and data analysis against historic data.	Migration effort is more complex than option 3 as a fourth target system is added to the scope. Development effort required to build/extend a reporting/ warehouse solution.
3	Existing legacy databases are taken offline and access to data is via reports (canned and ad-hoc) across the database.	Restricts the volume of data that requires migration. Restricts the volume of multiply migrated data records within new applications. Migration source retains intact for post migration audits and queries.	Once new application archiving solutions are implemented offline databases may require migration into the archiving solution.

16.4 Data Migration – Technical Considerations

While implementing data migration architecture, the data migration team has to take a number of considerations. Following are a few of such considerations:

- Data volume analysis
- Source system and target system processing power
- Complexity of data mapping rules and business rules

If during transformation, several records are normalized into separate database records that will result in a significant increase in the overall data volume, extract data from the source system(s) as is and move it to a staging area in the target system, then apply cleansing and transformations locally.

Highlights:

- Reduced network round trip
- Local transformations means the actual data migration process is over, data has actually reached the targeted server.
- Leverage processing power of target server

16.5 Data Migration Approach

The data migration process for IRDA Business Analytics Program will chiefly have three steps

- Conversion of data into electronic format
- Semantically or logically aligning data
- Transforming the data into physical formats

Following table illustrates the approach needs to be taken for the different combinations of physical and logical states of the data.

Logical State of Data →	Hardcopy	Excel	RDBMS
Physical Data Model	Physical Tabular Structure Paper Data	Physical Tabular Structure Excel based data	Physical Tabular Structure RDBMS storage
Conceptual Data Model	Conceptual level Structure Paper Data	Conceptual level Structure Excel based data	Conceptual level Structure RDBMS storage
Content	No Logical Structure Paper data	Conceptual level Structure Excel based data	Conceptual level Structure RDBMS storage

Physical State of Data →

Depending upon the state of data both logical and physical appropriate courses of actions needs to be taken.

16.6 Data and Document Migration Methodology

Pre – Migration Activities and Deliverables

Key activities:

- Identify data source and their details
- Run system extracts and queries
- Conduct user interviews and awareness programs on data migration process
- Review migration scope and validation strategy
- Create work plan and milestone dates
- Identify data cleansing needs and expectations
- Create data prep worksheets
- Clean up source data in current system
- Format unstructured data in other systems
- Run extracts and queries to determine data quality
- Create metrics to capture data volume, peak hours and off-peak hours

Deliverables/Outputs

- Migration scope document
- Migration validation strategy document
- Work plan with milestone dates

Data Cleansing

One of the main activities in this stage will be to clean the data to minimize data quality issues in the data sources.

A data quality issue can be categorised into two types:

1. A 'semantic' data quality issue in which data does not comply with 'As Is' business rules; or
2. A 'physical' data quality issue in which the data which does not comply with application rules, data definitions or validations in either existing source systems or new applications.

While there are synergies between migration and cleansing, there can be no. of challenges faced which are the following:

- Identification of 'semantic' data quality issues requires an in depth knowledge of the business domain which will required IRDA business users involvement
- Resolution of such quality issues requires subjective judgement which draws on business expertise.

- Many data quality issues require resolutions that are too complex to automate successfully through the backend and can only be fixed manually via the frontend application.
- Data migration is a critical activity which requires as stable a dataset as possible.
- Data migration must be complete before implementation, whereas only a small proportion of cleansing of 'semantic' quality issues are likely to be critical to the implementation and operation of the new system.

Invariably during the data migration life cycle, data quality issues will be identified that will prevent a successful migration. Therefore the Business Analytics data migration team will need to work with the data owners to facilitate resolutions for such issues. The data migration team will maintain a data quality issue register and pass any identified data quality issues back to the business owner for resolution. Each business unit impacted by the migration of the data from different sources will be required to identify a data quality champion to whom any the data quality issues can be referred and who will coordinate their resolution prior to the migration activity.

To allow the business the greatest lead time possible, the IRDA Business Analytics Program data migration team will conduct analysis across the dataset requiring migration to identify as many data quality issues that may impact the data migration process as early as possible in the life cycle

As part of the migration process data from the source systems may be 'transformed' to make it compatible with the target application. The data transformation logic may be able to fix simple 'physical' data quality issues such as:

- Removal of leading and trailing white space;
- Removal of illegal character types;
- Mapping of invalid codes to valid codes;
- Change of case e.g. upper to lower case; etc.

Migration Activities and Deliverables

Key Activities:

- Create/verify data element mappings
- Run data extracts from current system(s)
- Create tables, scripts, jobs to automate the extraction
- Address additional data clean-up issues
- Execute application specific customizations
- Run mock migrations
- Conduct internal data validation checks including business rules and referential integrity checks
- Perform data validation
- Prepare migration validation reports and data movement metrics
- Review migration validation reports and metrics
- Record count verifications on the new system
- Reconcile or resolve any exceptions or unexpected variations
- Sign off on migration validation

Deliverables/Outputs

- Extracts from source system
- Data migration modules, jobs, scripts
- New application(s) loaded with converted data
- Exceptions, alerts and error handling control points
- Exception reports, cross-reference files/manuals
- Signed-off data migration validation document

Post – Migration Activities and Deliverables

Key Activities

- Complete data migration reports and cross-reference files/manuals
- Data Archiving Strategy

Deliverables / Outputs

- Data archiving strategy document

16.7 Data Archiving Strategy

It is important to determine the specific level of controls necessary for each piece of data. Data should be classified into groups based on its value or sensitivity. The data classification process should define the information controls necessary to ensure appropriate confidentiality. IRDA should utilize an information classification program for their data as per **International Standard ISO -15489,** which describes requirements to identify, retain, and protect records used in the course of business to ensure integrity with proper handling.

Roles and Responsibilities

It is necessary to identify individuals by their authority and access requirements to implement policies, standards, and procedures. Three groups of authority are recommended in the context of Document Control and they are Owner, Custodian and User. It should be noted that the roles may be overlapping and an individual may simultaneously handle multiple roles.

Data Owner

The executives or managers should form this group responsible for the data content. Responsibilities include, but are not limited to the following:

- Data content verification
- Assign information classification level
- Assigning of appropriate controls
- Specify acceptable use of the data
- Identify appropriate users and the Data Custodian

Data User

This group consists of users who use the computerized data for various official purposes. These users may be internal or external to the organization. Responsibilities include, but are not limited to the following:

- Follow standards of acceptable use and compliance with the owner's controls
- Maintain confidentiality of the data and report unauthorized activity

Data Custodian

- Implementation of data storage safeguards and ensuring availability of the data is the primary responsibility of this group. This group should provide support to the business user(s). Responsibilities include, but are not limited to the following:

- Implement controls matching information classification
- Monitor data security for violations and administer user access controls
- Ensure data integrity through processing controls
- Back up data to protect from loss
- Act as a point of resolution for any confusion relating to data

For details of marking, transmission, storage, restoration, and destruction procedures / guidelines for information assets, please refer to Appendix G

16.8 Physical and Analog Data Conversion tools and techniques

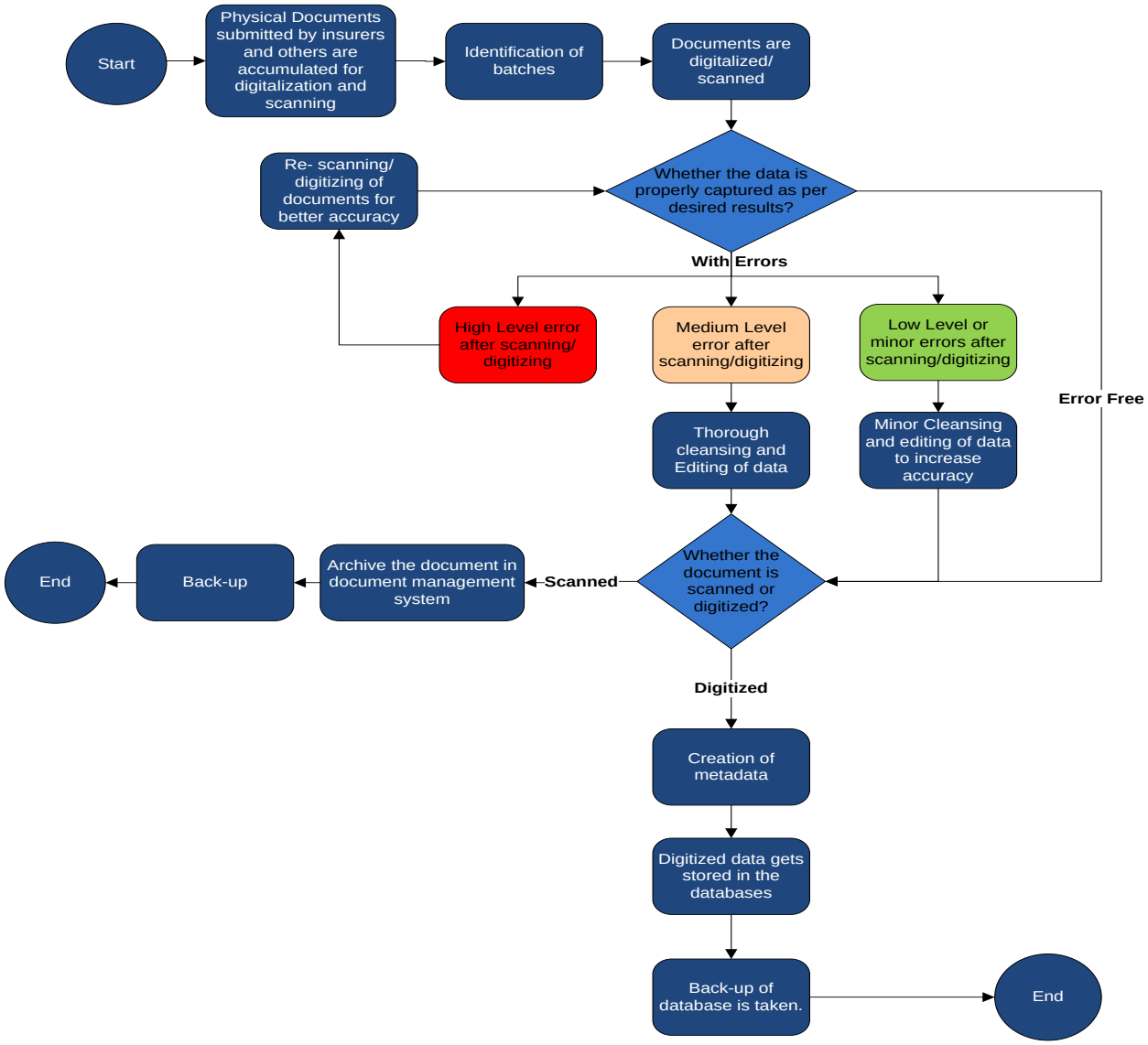
There are several tools and techniques available for converting physical analog data to electronic data. All the hardcopies of the document submitted as an attachment by the insurers and other users of the system in IRDA can be converted into electronic formats using these techniques. In the context of IRDA, two techniques are suggested:

- Manual data entry – This is the conventional and most prevalent technique and is applied by employing data entry operators who will on a regular basis for a certain time period in the implementation schedule will manually enter data using the hardcopy and the physical files in IRDA in a format prescribed during the design stage and finally the data will get stored in the system databases.
- Data Digitization and scanning – Digitization is a method of converting analog form of data to digital and electronic formats using advanced tools and technologies without the need of manual intervention. Scanning is a method of converting physical formats of data into electronic formats like images and PDFs etc. Data digitization and scanning in IRDA will involve the following processes:
    - Identification of the items for the collection – Identify which data are needed to be converted into digital formats. For example, actuarial report and abstract submitted by the insurer to the actuarial department.
    - Choice of formats – Deciding upon the formats to which these data is going to be converted. For example, *.doc, *.html, *.rtf etc.
    - Choice of hardware – Hardware infrastructure needed to convert this data to electronic format. For example, scanners, OCRs (Optical Character Readers), computers etc.
    - Choice of software – Selection of the software supporting digitization such as OCR and ICR.
    - Storage and archiving – Calculating the storage space required for the digitized data.
    - Management – Managing the activities so as to ensure optimal results. There several factors to be kept in mind for getting the desired quality for digitization such as conditions and coloring of the source documents, font types, persons handling the

activities etc. along with unknown factors. All these needs to be managed while managing the entire activity of digitization

Following diagram is a representation of the workflow of the manual data conversion activities to be carried out in IRDA.

IRDA Physical Data Conversion Workflow



16.9 Risks and challenges in Data Migration

Key Risks and Challenges

The success of the data migration project lies in a seamless data movement and always remains on the shadow of implementing the new system.[3]

Following are few common risks involved in a data migration process.

Failure to treat data migration as a project unto itself. Data migration is complex undertaking that should not be regarded as merely a peripheral effort to the main development project. The data migration effort should be treated as a complete sub-project with a defined process, a thoughtfully derived time and cost estimate, and a series of phases that can be tracked or managed.

Underestimating the time and cost of data migration. It is important to perform a reasonably diligent survey of source systems in order to determine the quality of those source system's documentation and source data. If the source system does not have up-to-date data documentation in the form of data model and data dictionary, the task of determining the structure and data types of the desired source data and it's mapping to the target data will be increased in time and cost. If the source system has less stringent data quality requirements than the target system or if the data quality of the source system has been allowed to lapse over time, the actual act of performing the migration will take longer time due to the need to perform post-migration data clean up.

Lack of end-state data quality. If the migration effort does not formally specify the level of end-state data quality and the set of quality control tests that will be used to verify that data quality, the target domain may wind up with poor data quality. This will negatively impact the perceived outcome of the development effort.

Failure to support the organizational support. When the complexity and importance of data migration is not adequately appreciated it may be difficult to gain organizational support for that data migration, especially in terms of funding and resources. It may be even more difficult to garner a positive level support in separate organizations that have primary responsibility for the source data. This can happen when the organization supporting the source data feels threatened by the new system or it can happen simply because the migration effort is not a top priority for that organization.

Lack of appreciation for the complexities of data mapping. The central effort of data migration is understanding the source data and developing the mapping that allows the data in the source domain to be accurately transformed and moved to the target domain. There are many factors affecting mapping that can be ignored:

- Ensuring that the semantics sense of a given attribute is correctly mapped: the same datum may carry a different name in the source domain than in the target domain; the source domain and the target domain may carry the same name for what is conceptually a different datum.

[3] For details of risks related to Business Analytics Project, please refer to "Risk Mitigation Strategy" section of the implementation plan document

- Understanding that the number of entities and their respective relationships may be vastly different between the source domain and the target domain.
- Strategies and extensions may have to be developed to handle certain intractable mappings if they are discovered. An attribute may exit in the source domain that does not exist in the target domain and vice versa.

These issues and subsequent impacts may manifest themselves in both quantitative and qualitative ways:

In quantitative sense this can result in:

- Costs associated with error detection
- Costs associated with error rework
- Costs associated with error prevention
- Time delays in operations
- Costs associated with delays in processing

In a qualitative sense this can result in:

- Difficult and/or erroneous decisions
- Organization wide data inconsistency
- Low acceptance level by users of the new system

Risks Mitigation Process

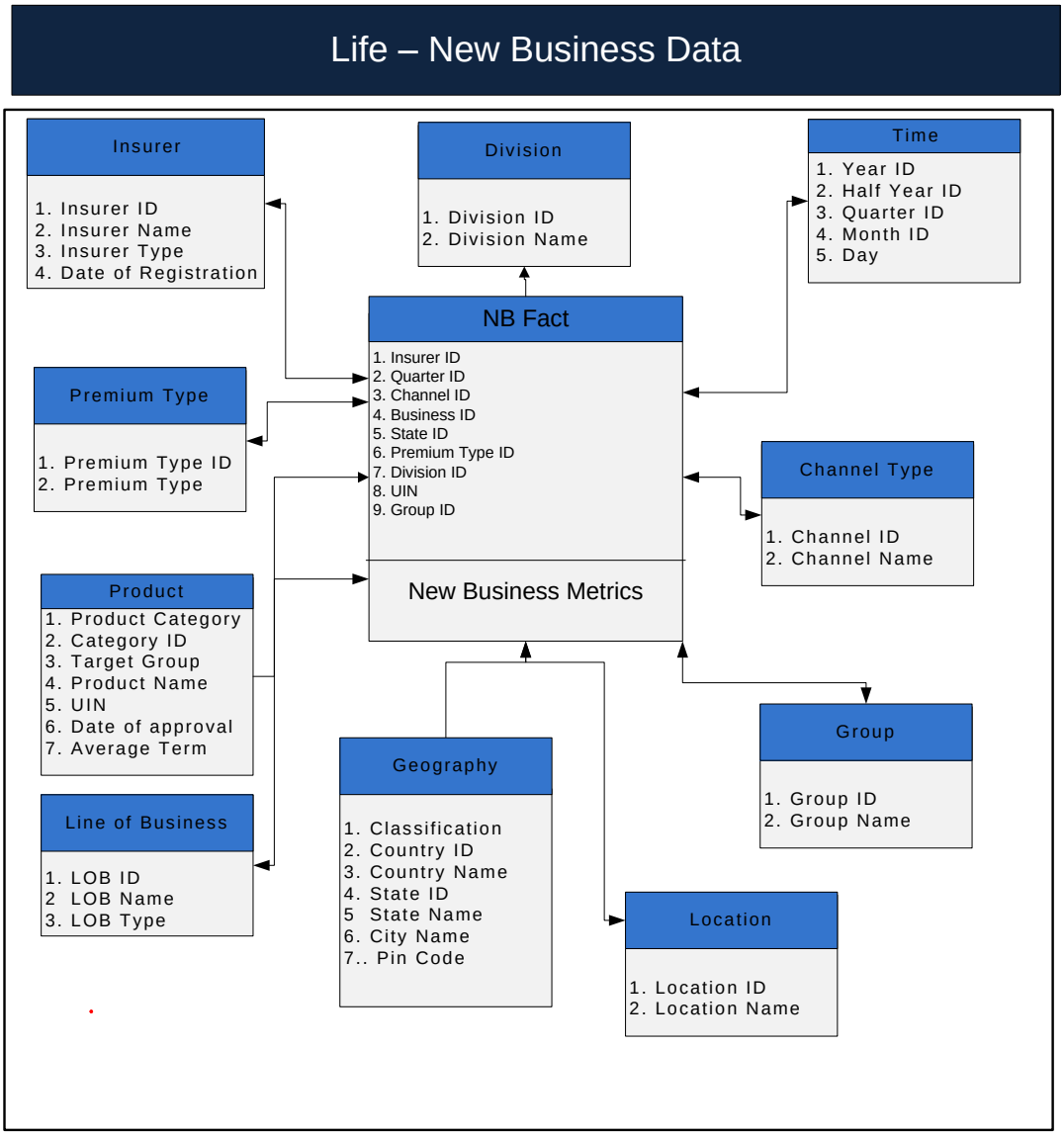
The most important factors in mitigating the risks of data migration are to treat the data migration as a project and to use a sound methodical process having the following KPIs:

- **Data Profiling -** Gain a complete understanding of the content, structure, quality, and integrity of the data of the source system.
- **Data Mapping -** Develop an accurate set of data mapping specifications from the source system to the target system.
- **Migration Approach and Architectural Considerations -** Whether point-to-point migration or hub-and-spoke migration, this needs to be evaluated and carefully articulated.
- **Development –** Selecting a tool to automate the migration process and make it more scalable should be a high-priority item.
- **Quality Assurance -** Conduct mock migrations, pilot migrations before the final migration run; this will ensure that the migration process is robust and trusted.

Appendix

A. Department wise data model

1. Life Department



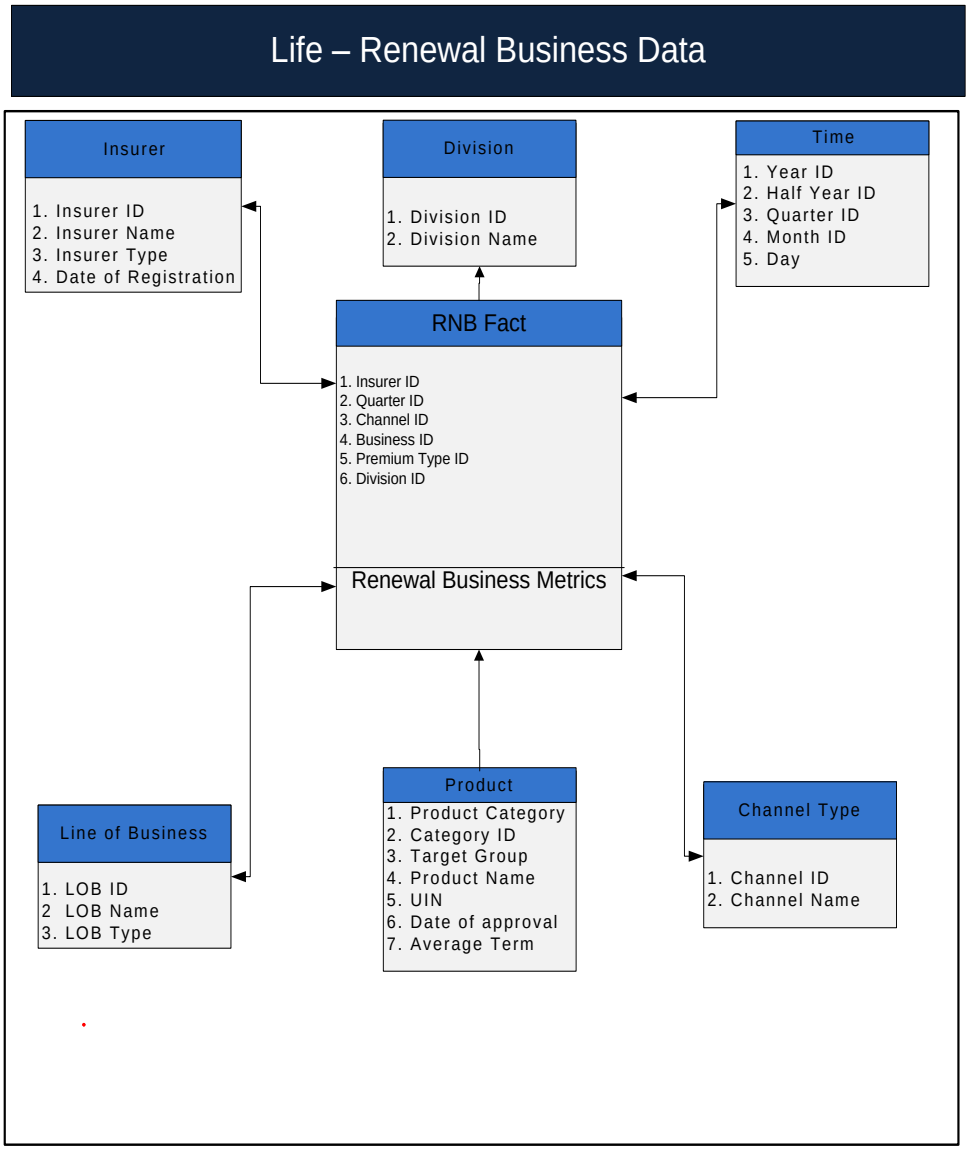
Associated Forms (Life-Department)			
Code	**Form Name**	**Objective**	**Frequency**
INPUT_LIFE_9	New Business Data - Channel wise	To capture the new business data against all channels at an overall level	Quarterly
INPUT_LIFE_9.1	New Business Data - Product and Channel Wise	To capture the new business data for each channel and product	Yearly
INPUT_LIFE_10	New Business Data - State wise	To capture data on new business across states for individual and group business.	Quarterly
INPUT_LIFE_12	Group New Business Category wise Data	To capture information on New Business - (single premium and regular premium) for different schemes of group business	Quarterly
INPUT_LIFE_11(b)	Business Data on Social Security Schemes	To capture data on Social Security Schemes funded/subsidized by Government of India/State Government	Yearly
INPUT_LIFE_9.2	New Business - Commissions Data	To capture the commissions expenses data for an insurer	Yearly
INPUT_LIFE_14	Details of New Business Data For MI - Channel wise	To capture data on new business against all the micro insurance channels along with no. of total existing MI products.	Quarterly
INPUT_LIFE_14.1	Details of New Business Data For MI - Product and Channel wise	To capture data on new business for each MI product and channel type	Yearly
INPUT_LIFE_14(a)	New Business Data For MI - State wise	To captures the state wise break up of MI New Business Data	Quarterly

Similar Forms from Other Departments (F&A-Department)			
Code	**Form Name**	**Objective**	**Frequency**
INPUT_FnA_LIFE_NBS	New Business Data for Life Department	To capture the new business data for life insurance products	Monthly
INPUT_FnA_LIFE_SCHEDULE2	Commission Expenses – Line of Business Wise	To capture the detailed breakup of the commission expense for each line of business	Yearly

Dept.	Form Name	Dimensions									
		Insurer	Product	LoB	Premium Type	Division	Channel	Geography	Group	Location	Time
Life	New Business Data - Channel wise	X	C	X	X	X	X				Q
	New Business Data - Product and Channel Wise	X	P	X	X	X	X				Y
	New Business Data - State wise	X	C	X	X	X		X			Q
	Group New Business Category wise Data	X	C	X	X			X			Q
	Business Data on Social Security Schemes	X	P	X	X			X			Q
	New Business - Commissions Data	X	C	X	X		X				Y
	Details of New Business Data For MI - Channel wise	X				X	X				Q
	Details of New Business Data For MI - Product and Channel wise	X	P			X	X				Y
	New Business Data For MI - State wise	X				X		X			Q
F&A	New Business Data for Life Department	X	C	X	X	X			X	X	M
	Commission Expenses – Line of Business Wise	X		X			X				Y

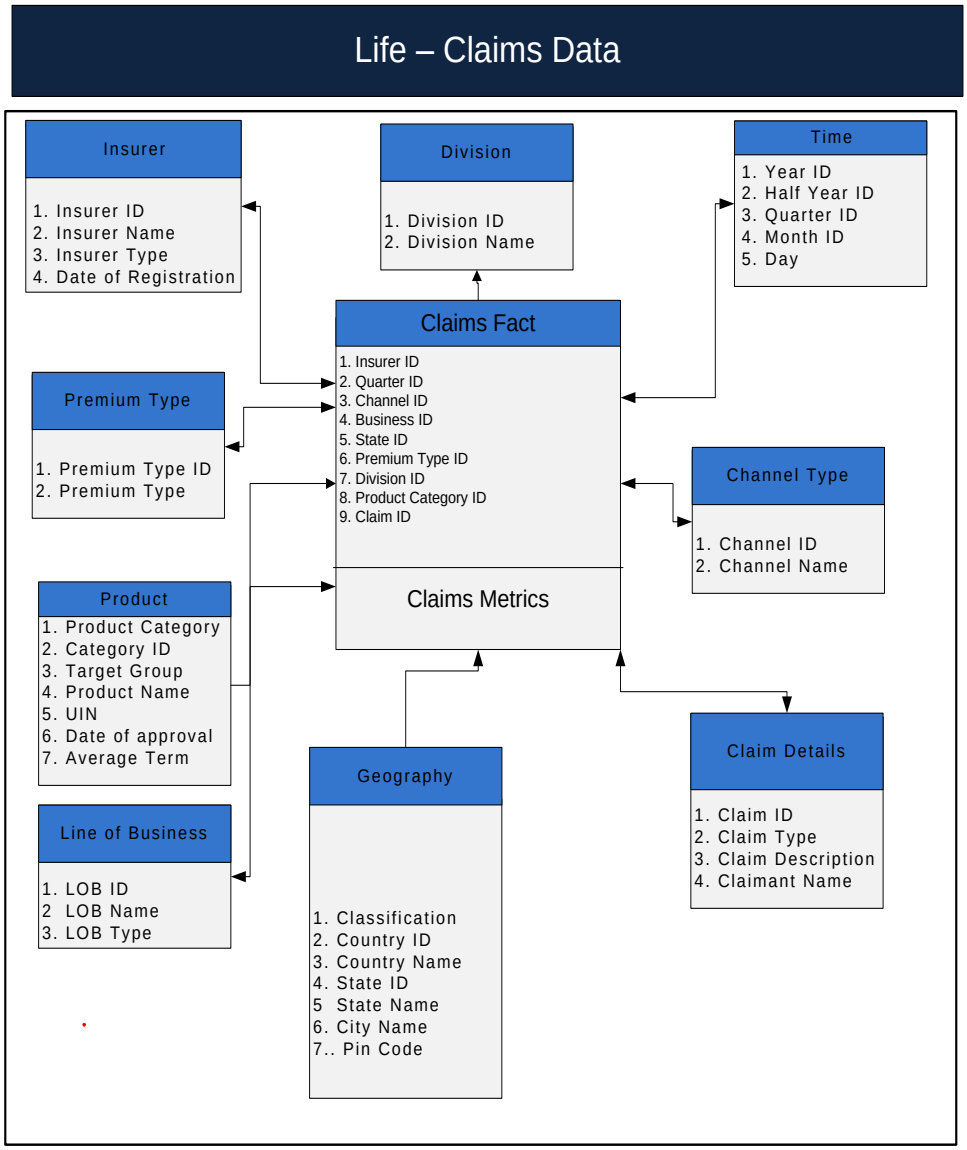
C: Category Level; P: Product level

M: Monthly; Q: Quarterly; Y: Yearly


Life – Renewal Business Data
Insurer
1. Insurer ID
2. Insurer Name
3. Insurer Type
4. Date of Registration
Division
1. Division ID
2. Division Name
Time
1. Year ID
2. Half Year ID
3. Quarter ID
4. Month ID
5. Day
RNB Fact
1. Insurer ID
2. Quarter ID
3. Channel ID
4. Business ID
5. Premium Type ID
6. Division ID
Renewal Business Metrics
Line of Business
1. LOB ID
2 LOB Name
3. LOB Type
Product
1. Product Category
2. Category ID
3. Target Group
4. Product Name
5. UIN
6. Date of approval
7. Average Term
Channel Type
1. Channel ID
2. Channel Name

Associated Forms (Life Department)			
Code	**Form Name**	**Objective**	**Frequency**
INPUT_LIFE_9.3	Renewal Business Data - Product and Channel Wise	To capture the renewal business data for each channel and product	Yearly
INPUT_LIFE_9.4	Renewal Business Data - Channel wise	To capture the new business data against all channels and sub-segments (rural ,urban, semi urban and metro)	Quarterly

Dept.	Form Name	Dimensions					
		Insurer	Product	LoB	Division	Channel	Time
Life	Renewal Business Data - Product and Channel Wise	X	P	X	X	X	Y
	Renewal Business Data - Channel wise	X	C	X	X	X	Q


Life – Claims Data
Insurer
1. Insurer ID
2. Insurer Name
3. Insurer Type
4. Date of Registration
Division
1. Division ID
2. Division Name
Time
1. Year ID
2. Half Year ID
3. Quarter ID
4. Month ID
5. Day
Claims Fact
1. Insurer ID
2. Quarter ID
3. Channel ID
4. Business ID
5. State ID
6. Premium Type ID
7. Division ID
8. Product Category ID
9. Claim ID
Claims Metrics
Premium Type
1. Premium Type ID
2. Premium Type
Channel Type
1. Channel ID
2. Channel Name
Product
1. Product Category
2. Category ID
3. Target Group
4. Product Name
5. UIN
6. Date of approval
7. Average Term
Line of Business
1. LOB ID
2 LOB Name
3. LOB Type
Geography
1. Classification
2. Country ID
3. Country Name
4. State ID
5 State Name
6. City Name
7.. Pin Code
Claim Details
1. Claim ID
2. Claim Type
3. Claim Description
4. Claimant Name

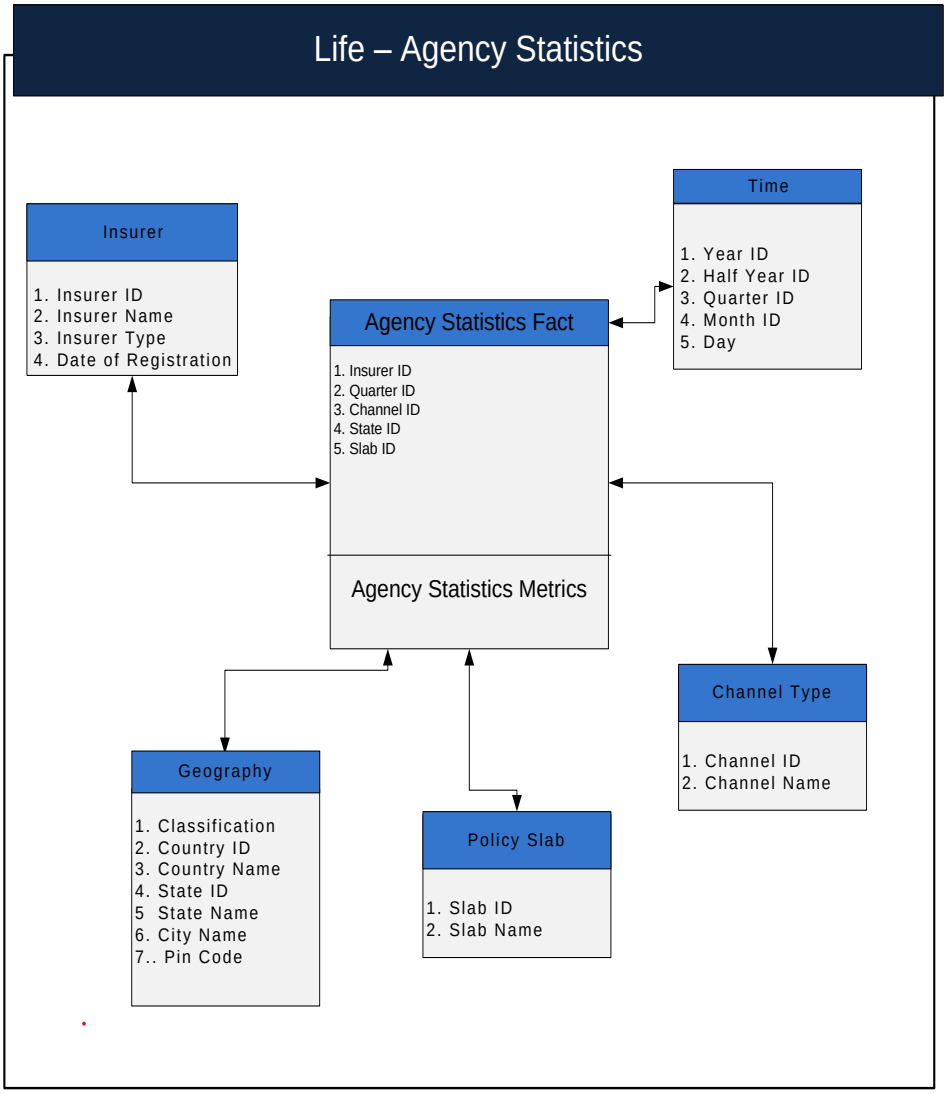
Associated Forms (Life Department)			
Code	**Form Name**	**Objective**	**Frequency**
INPUT_LIFE_11(a)	Claims Data on Social Security Schemes	To collect the state wise claims information on social security schemes	Quarterly
INPUT_LIFE_16	Survival/Periodic Benefits and Maturity Benefits (Individual)	To capture the data on survival/periodic and maturity benefits under individual business	Quarterly
INPUT_LIFE_17(a)	Death Claims (Individual)	To capture the data on death claims for individual business	Quarterly
INPUT_LIFE_17(b)	Death Claims (Group)	To capture the data on death claims for group business	Quarterly
INPUT_LIFE_17©	Rider Claims Data	To capture the data on rider claims for individual business	Quarterly
INPUT_LIFE_18	State wise Death Claims Movement Form	To capture the claims data for each state for both individual and group business	Quarterly
INPUT_LIFE_18.2	Details of Claims Handled through TPAs	To capture the movement of claims handled through TPA	Quarterly
INPUT_LIFE_19(a)	MI Claims Movement Form – Maturity	To capture the claims data for MI business – Maturity only	Quarterly
INPUT_LIFE_19(b)	MI Claims Movement Form - Death Claims	To capture the claims data for MI business – Death claims only	Quarterly
INPUT_LIFE_20	Penal Interest Paid - Claims and Benefits	To capture the data on penal interest paid to policyholders.	Quarterly
INPUT_LIFE_21	Health Claims	To capture data for health claims	Quarterly

Associated Forms (Life Department)			
Code	**Form Name**	**Objective**	**Frequency**
	Data		
INPUT_LIFE_23	Repudiated Claims Data	To capture claim wise details for each instance of repudiation	Quarterly

Similar Forms from Other Departments (Non Life Department)			
Code	**Form Name**	**Objective**	**Frequency**
INPUT_NONLIFE_ Pending_Claims	Claims pending for more than six months and repudiated claims	To capture claim wise details for each instance of repudiation and pendency for more than 6 months	Quarterly

Dept.	Form Name	Dimensions								
		Insurer	Product	LoB	Premium Type	Division	Channel	Geography	Claim Details	Time
Life	Claims Data on Social Security Schemes	X	P	X				X		Q
	Survival/Periodic Benefits and Maturity Benefits (Individual)	X	C	X		X			X	Q
	Death Claims (Individual)	X	C	X		X			X	Q
	Death Claims (Group)	X	C	X		X			X	Q
	Rider Claims Data	X							X	Q
	State wise Death Claims Movement Form	X				X		X	X	Q
	Details of Claims Handled through TPAs	X							X	Q

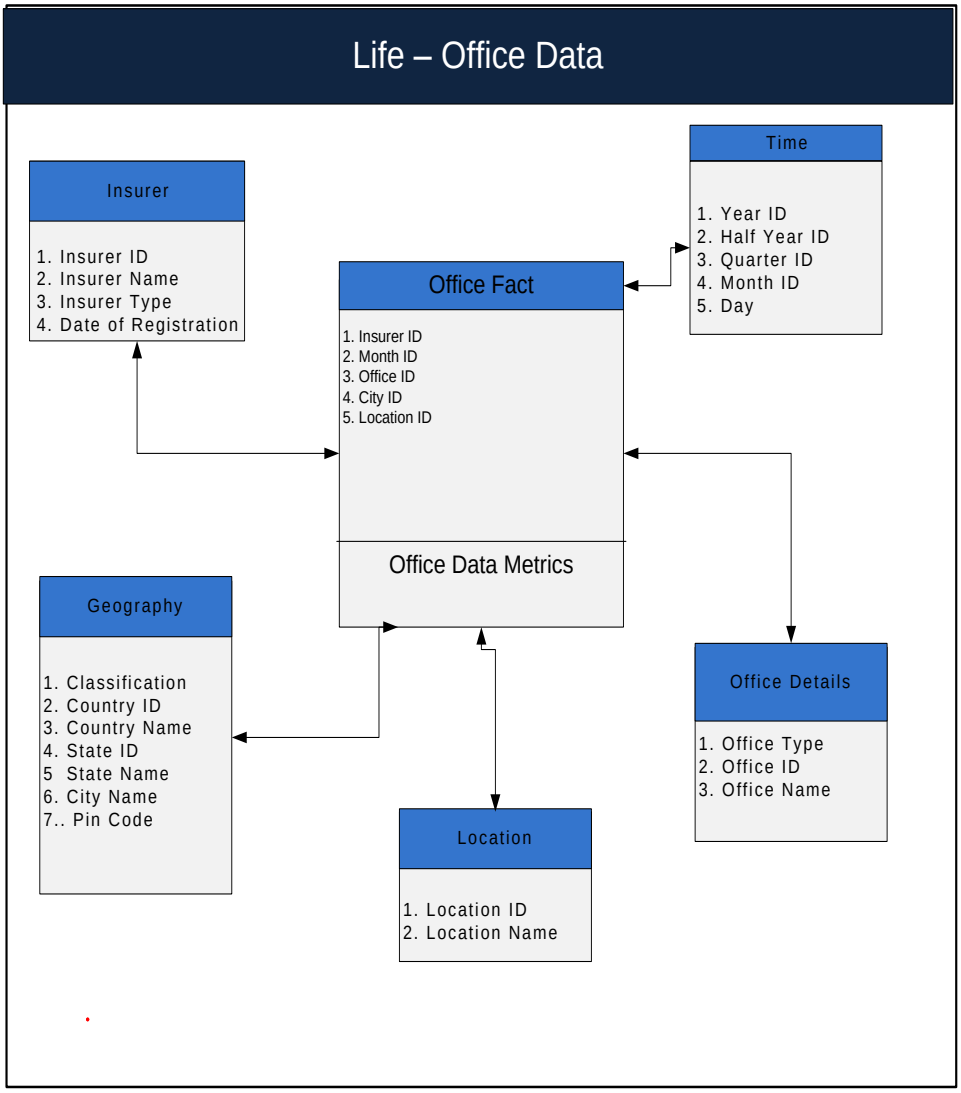
Dept.	Form Name	Dimensions								
		Insurer	Product	LoB	Premium Type	Division	Channel	Geography	Claim Details	Time
	MI Claims Movement Form – Maturity	X							X	Q
	MI Claims Movement Form - Death Claims	X				X			X	Q
	Penal Interest Paid - Claims and Benefits	X							X	Q
	Health Claims Data	X							X	Q
	Repudiated Claims Data	X	P						X	Q
Non Life	Claims pending for more than six months and repudiated claims	X	P						X	Q


Life – Agency Statistics
Insurer
1. Insurer ID
2. Insurer Name
3. Insurer Type
4. Date of Registration
Time
1. Year ID
2. Half Year ID
3. Quarter ID
4. Month ID
5. Day
Agency Statistics Fact
1. Insurer ID
2. Quarter ID
3. Channel ID
4. State ID
5. Slab ID
Agency Statistics Metrics
Channel Type
1. Channel ID
2. Channel Name
Geography
1. Classification
2. Country ID
3. Country Name
4. State ID
5 State Name
6. City Name
7.. Pin Code
Policy Slab
1. Slab ID
2. Slab Name

Associated Forms (Life Department)			
Code	**Form Name**	**Objective**	**Frequency**
INPUT_LIFE_1	Agency Statistics Data	To capture the data on movement of agents during the year for each insurer	Quarterly
INPUT_LIFE_1.3	Agency Statistics Data – Slab Wise	To capture the detailed breakup of the agents based on different policy slabs	Quarterly
INPUT_LIFE_1(a)	Agency Statistics Data – State wise	To capture the data on no. of agents at the end of quarter for each state.	Quarterly
INPUT_LIFE_1(b))	Micro Insurance Agency Statistics Data	To capture the data on movement of MI agents during the year for each insurer	Quarterly
INPUT_LIFE_1(c)	Micro Insurance Agency Statistics Data - State wise	To collect the data on no. of MI agents at the end of quarter for each state.	Quarterly

Dept.	Form Name	Dimensions				
		Insurer	Geography	Channel Type	Time	Policy Slab
Life	Agency Statistics Data	X		X	Q	X
	Agency Statistics Data – Slab Wise	X		X	Q	X
	Agency Statistics Data – State wise	X	X	X	Q	

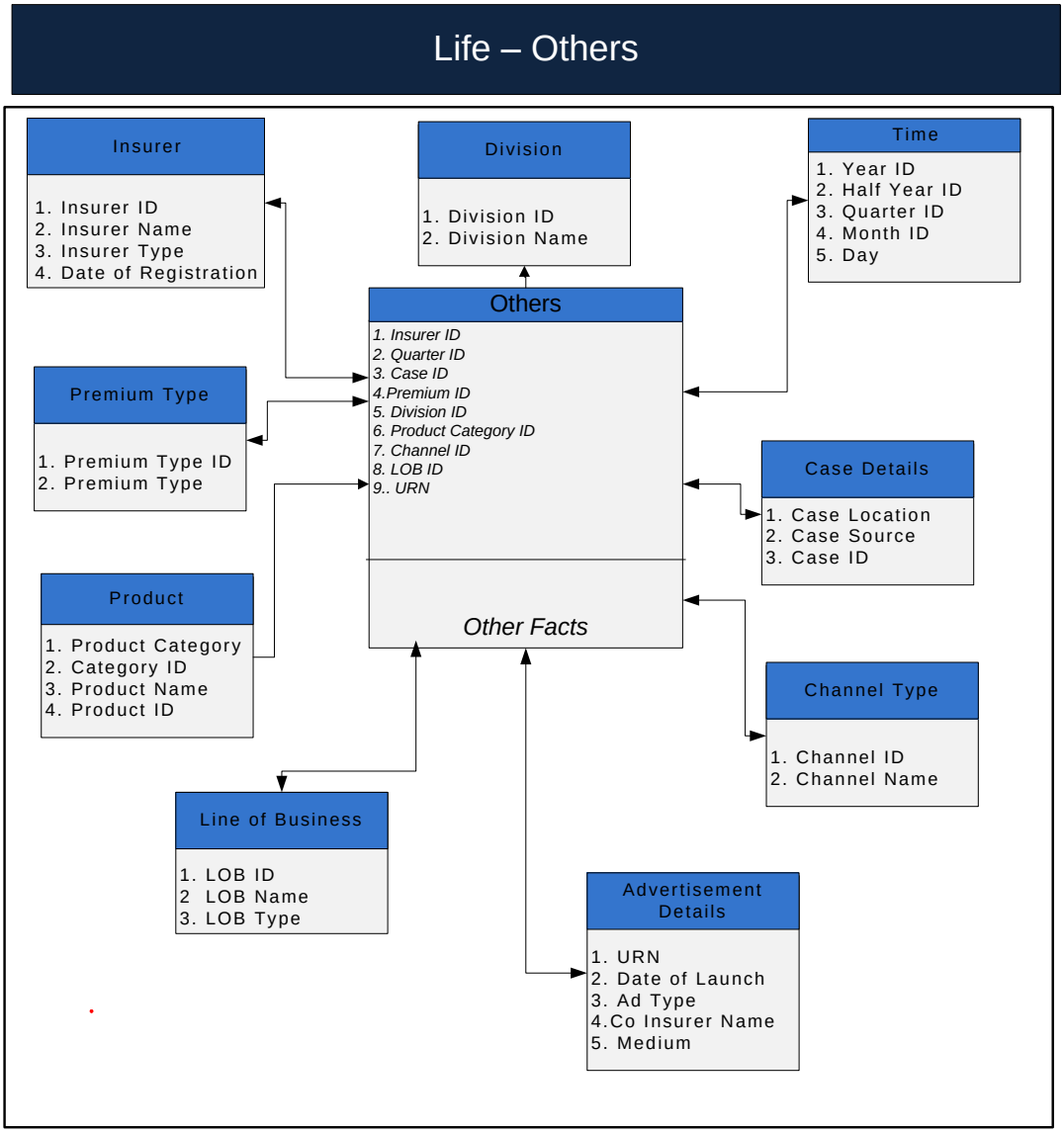
Dept.	Form Name	Dimensions				
		Insurer	Geography	Channel Type	Time	Policy Slab
	Micro Insurance Agency Statistics Data	X		X	Q	
	Micro Insurance Agency Statistics Data - State wise	X	X	X	Q	


Life – Office Data
Insurer
1. Insurer ID
2. Insurer Name
3. Insurer Type
4. Date of Registration
Time
1. Year ID
2. Half Year ID
3. Quarter ID
4. Month ID
5. Day
Office Fact
1. Insurer ID
2. Month ID
3. Office ID
4. City ID
5. Location ID
Office Data Metrics
Geography
1. Classification
2. Country ID
3. Country Name
4. State ID
5 State Name
6. City Name
7.. Pin Code
Location
1. Location ID
2. Location Name
Office Details
1. Office Type
2. Office ID
3. Office Name

Associated Forms (Life Department)			
Code	**Form Name**	**Objective**	**Frequency**
INPUT_LIFE_2	New Office Application Form (Online)	Each insurer who seeks to open new offices will have to fill up the form for approval of IRDA	As and When
INPUT_LIFE_2(a)	Intimation of opening/ relocation/closure of offices	Insurers are required to inform IRDA about opening/relocation/closure of offices in the reporting month.	Monthly
INPUT_LIFE_4	Office Statistics Data – State Wise	To capture the movement of no. of offices for an insurer state wise.	Quarterly

Similar Forms from Other Departments (Non Life Department)			
Code	**Form Name**	**Objective**	**Frequency**
INPUT_NON_LIFE_ **Office_1**	OFFICE DETAILS	To collect the information on the office (Branch) details in each state for each insurer.	Quarterly
INPUT_NON_LIFE_Office_1.1	Details of foreign offices	To capture the information on the foreign offices classified as representative offices, branches, subsidiaries, agency offices	Quarterly

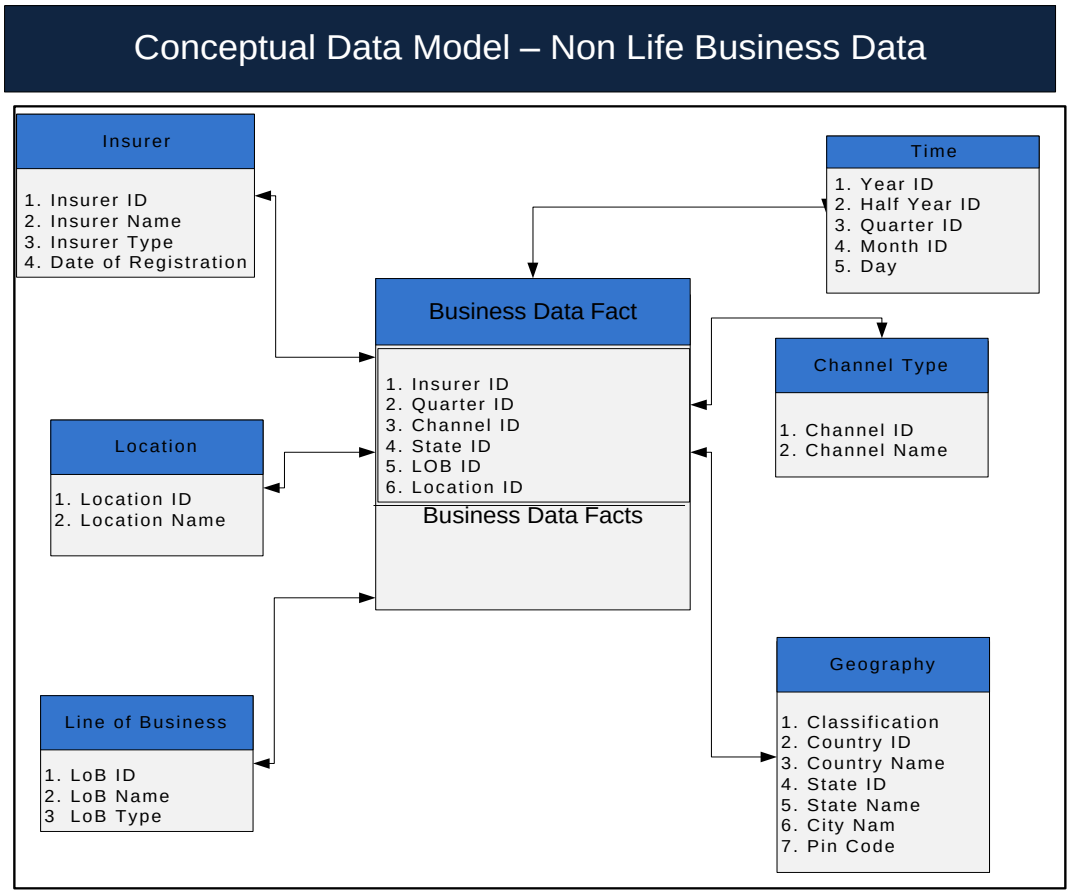
Dept.	Form Name	Dimensions				
		Insurer	Geography	Office Details	Time	Location
Life	New Office Application Form (Online)	X	X	X	D	X
	Intimation of opening/ relocation/closure of offices	X	X	X	M	X
	Office Statistics Data – State Wise	X	X		M	X
Non Life	OFFICE DETAILS	X	X		Q	
	Details of foreign offices	X	X		Q	


Life – Others
Insurer
1. Insurer ID
2. Insurer Name
3. Insurer Type
4. Date of Registration
Division
1. Division ID
2. Division Name
Time
1. Year ID
2. Half Year ID
3. Quarter ID
4. Month ID
5. Day
Others
1. Insurer ID
2. Quarter ID
3. Case ID
4.Premium ID
5. Division ID
6. Product Category ID
7. Channel ID
8. LOB ID
9.. URN
Other Facts
Premium Type
1. Premium Type ID
2. Premium Type
Case Details
1. Case Location
2. Case Source
3. Case ID
Product
1. Product Category
2. Category ID
3. Product Name
4. Product ID
Channel Type
1. Channel ID
2. Channel Name
Line of Business
1. LOB ID
2 LOB Name
3. LOB Type
Advertisement Details
1. URN
2. Date of Launch
3. Ad Type
4.Co Insurer Name
5. Medium

Associated Forms (Life Department)			
Code	**Form Name**	**Objective**	**Frequency**
INPUT_LIFE_5(a)	Premium Awaited Policies (For the quarter)	To capture the details of the premium awaited policies for a particular quarter	Quarterly
INPUT_LIFE_5(b)	Premium Awaited Policies (For the quarter)	To capture the details of the premium awaited policies up to a particular quarter	Quarterly
INPUT_LIFE_6	Data on legal cases for an insurer	To capture movement of no. of legal cases during a particular period for an insurer	Quarterly
INPUT_LIFE_7	Details of Advertisements Released	To capture detailed level information of the advertisements those are released.	Monthly
INPUT_LIFE_7(a)	Details of Advertisements Filed for Approval - Joint Sales Advertisement	To capture the detailed level information of the joint sales advertisements	As and When
INPUT_LIFE_13	Data for surrenders, partial withdrawals, switches and top-ups.	To capture the information on surrenders, partial withdrawals, switches and top-ups.	Quarterly
INPUT_LIFE_22	Free Look and Cheque dishonor data	To collect data on free look and cheque dishonor data during the quarter.	Quarterly
INPUT_LIFE_24	Persistency Data	To capture persistency data for an insurer channel wise	Quarterly

Dept.	Form Name	Dimensions								
		Insurer	Product	LoB	Premium Type	Division	Channel	Advertisement Details	Case Details	Time
Life	Premium Awaited Policies (For the quarter)	X	C				X			Q
	Premium Awaited Policies (Up to the quarter)	X	C				X			Q
	Data on legal cases for an insurer	X							X	Q
	Details of Advertisements Released	X						X		M
	Details of Advertisements Filed for Approval - Joint Sales Advertisement	X						X		
	Data for surrenders, partial withdrawals, switches and top-ups.	X	C	X	X					Q
	Free Look and Cheque dishonor data	X					X			Q
	Persistency Data	X	C	X			X			Q

2. Non Life Department



Associated Forms (Non-Life-Department BS Data)			
Code	**Form Name**	**Objective**	**Frequency**
INPUT_NON_LIFE_PREMIUM_1	Segment wise Gross Premium data across all Channels - For the quarter	To collect Segment wise and State wise information on Gross Premium, No. of Policies and Total Sum Assured across Channels of Non-Life General business	Quarterly
INPUT_NON_LIFE_PREMIUM_1.1	Segment wise Gross Premium data across all Channels - Upto the quarter	To collect Segment wise and State wise information on Gross Premium, No. of Policies and Total Sum Assured across Channels of Non-Life General business	Quarterly
INPUT_NON_LIFE_PREMIUM_2	Segment wise direct business - Upto the quarter	To collect Segment wise and State wise information on Gross Premium, No. of Policies and Total Sum Assured for direct business	Quarterly
INPUT_NON_LIFE_PREMIUM_2.1	Segment wise direct business - For the quarter	To collect Segment wise and State wise information on Gross Premium, No. of Policies and Total Sum Assured for direct business	Quarterly

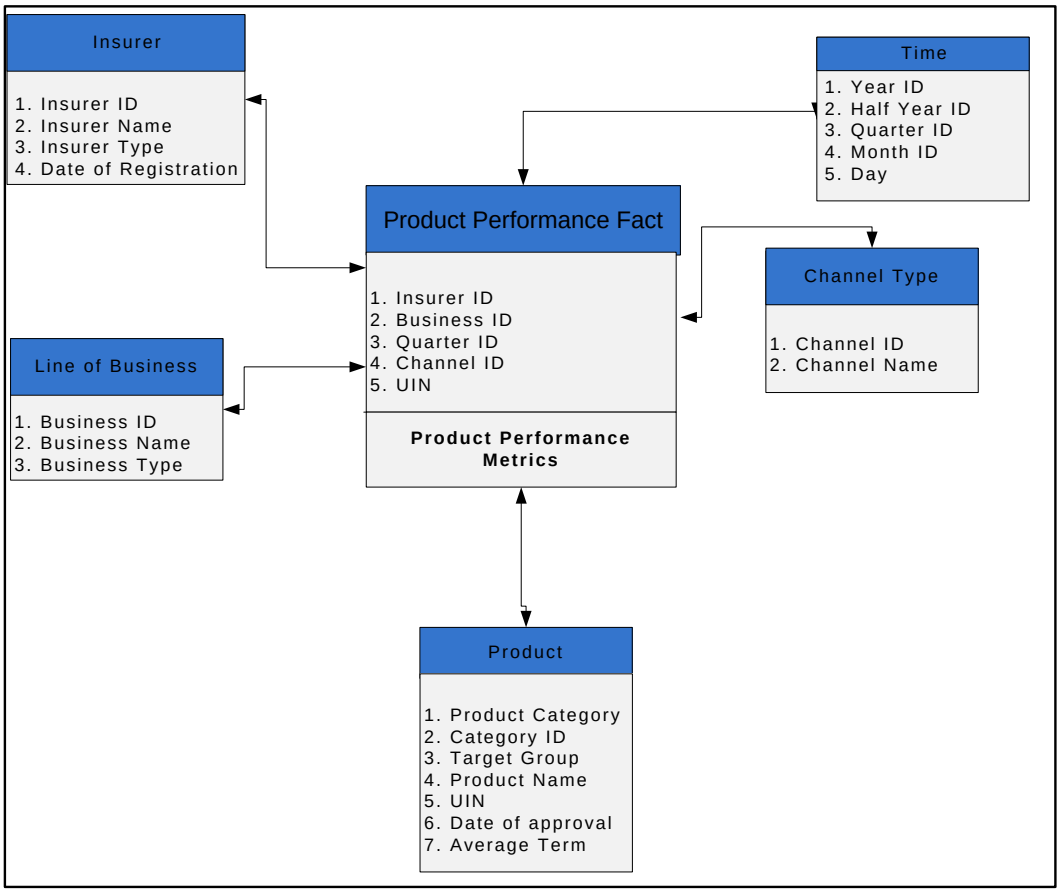
Similar Forms from Other Departments (F&A-Department)-			
Code	**Form Name**	**Objective**	**Frequency**
INPUT_FnA_NON LIFE_NBS	New Business Data for Non Life Department	To capture the new business data for non life insurance products	Monthly

Dept.	Form Name	Dimensions					
		Insurer	LoB	Channel	Geography	Time	Location
Non Life	Segment wise Gross Premium data across all Channels - For the quarter	X	X	X	X	Q	
	Segment wise Gross Premium data across all Channels - Upto the quarter	X	X	X	X	Q	
	Segment wise direct business - Upto the quarter	X	X	X	X	Q	
	Segment wise direct business - For the quarter	X	X	X	X	Q	
FnA	New Business Data for Non Life Department	X	X	X	X	M	X

C: Category Level; P: Product level

M: Monthly; Q: Quarterly; Y: Yearly

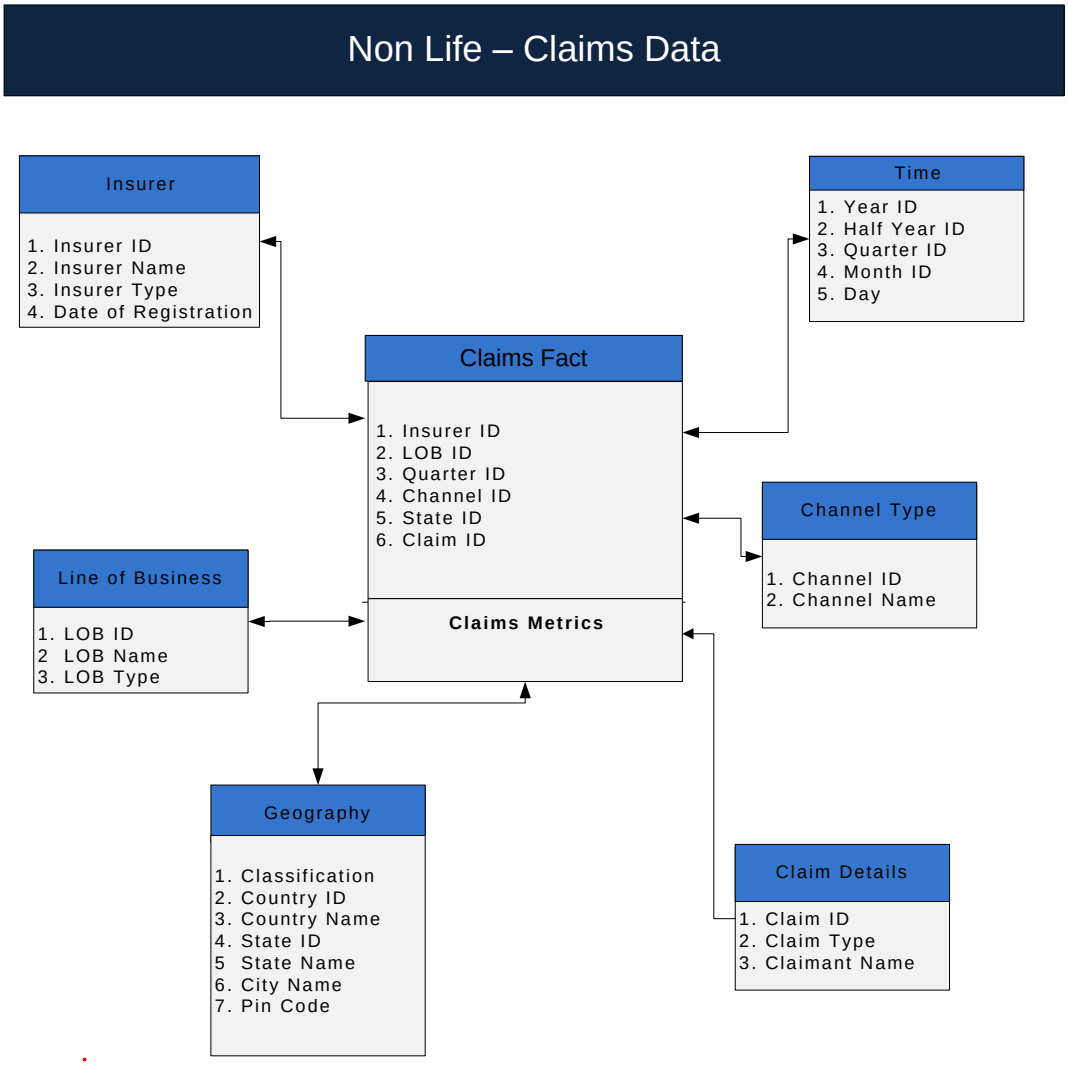
Conceptual Data Model for Non-Life – Product Performance Analysis



Associated Forms (Non-Life Department-Product Performance Analysis)			
Code	**Form Name**	**Objective**	**Frequency**
INPUT_NONLIFE_PDTPERF1.0	Details of product performance for products with 1 year contract	To collect product information for each product launched during the year.	Yearly and as and when required
INPUT_NONLIFE_PDTPERF2.0	Details of product performance for products with more than 1 year contract	To collect product information for each product launched during the year.	Yearly and as and when required
INPUT_NONLIFE_PDTPERF3.0	Details of product performance in terms of claims development and aging (To be furnished by All insurers having non-life products)	To collect claims movement and claims aging data for each product launched during the year.	Quarterly
INPUT_NONLIFE_PDTPERF4.0	Details of product performance in terms of channels (To be furnished by All insurers having non-life products)	To capture the performance of the products in terms of distribution channels	Yearly and as and when required

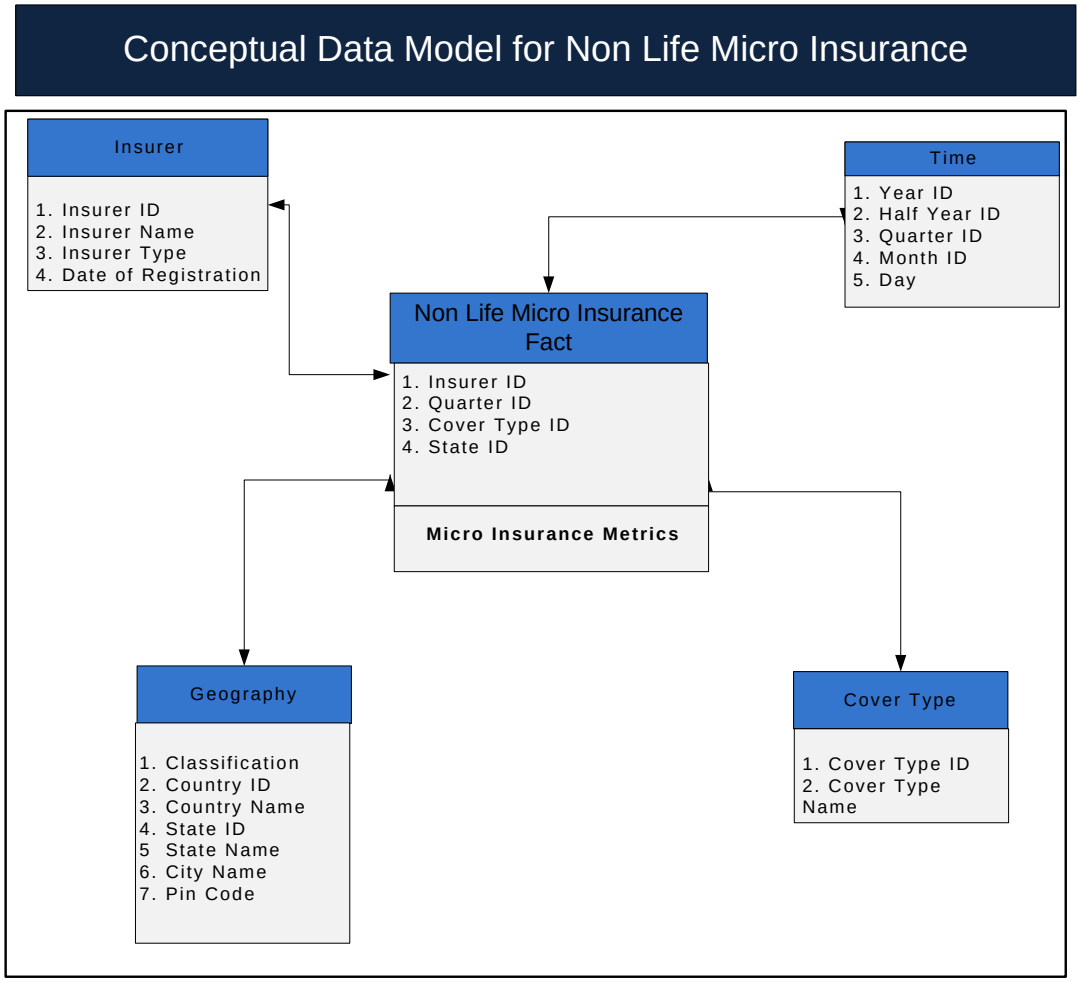
Similar Forms from Other Departments (F&A Department)			
Code	**Form Name**	**Objective**	**Frequency**
INPUT_FnA_NonLife_Schedule3	Details of commissions expenses	To collect commissions expenses for non life insurers	Yearly

Dept.	Form Name	Dimensions				
		Insurer	Product	LoB	Channel	Time
Non Life	Details of product performance for products with 1 year contract	X	P	X	X	Y
	Details of product performance for products with more than 1 year contract	X	P	X	X	Y
	Details of product performance in terms of claims development and aging (To be furnished by All insurers having non-life products)	X	P			Q
	Details of product performance in terms of channels (To be furnished by All insurers having non-life products)	X	P		X	Y
FnA	Details of commissions expenses	X		X		Y


Non Life – Claims Data
Insurer
1. Insurer ID
2. Insurer Name
3. Insurer Type
4. Date of Registration
Time
1. Year ID
2. Half Year ID
3. Quarter ID
4. Month ID
5. Day
Claims Fact
1. Insurer ID
2. LOB ID
3. Quarter ID
4. Channel ID
5. State ID
6. Claim ID
Claims Metrics
Channel Type
1. Channel ID
2. Channel Name
Line of Business
1. LOB ID
2 LOB Name
3. LOB Type
Geography
1. Classification
2. Country ID
3. Country Name
4. State ID
5 State Name
6. City Name
7. Pin Code
Claim Details
1. Claim ID
2. Claim Type
3. Claimant Name

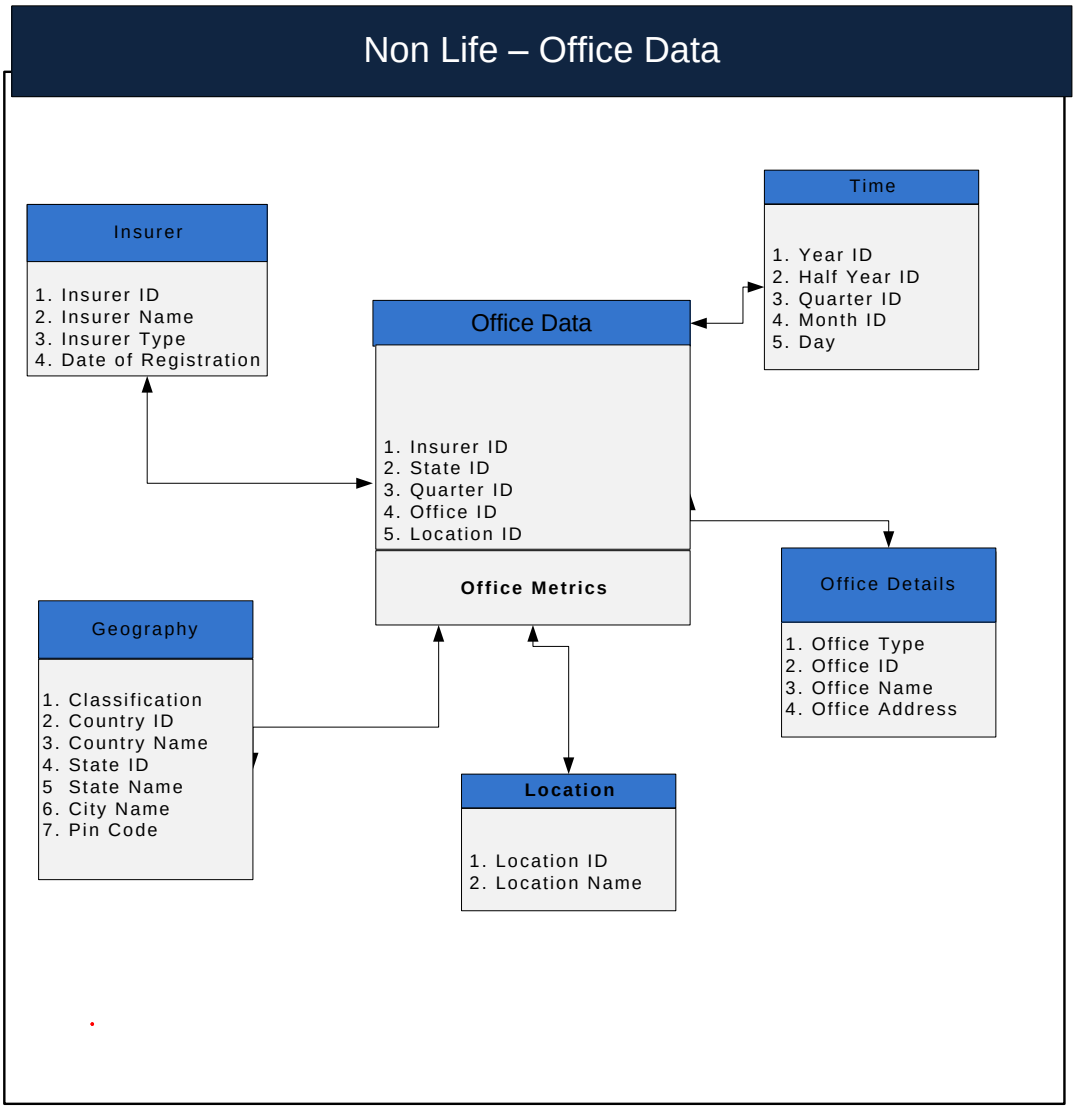
Associated Forms (Non-Life Department- Claims Data)			
Code	**Form Name**	**Objective**	**Frequency**
INPUT_NON_LIFE_CLAIMS_1	State wise and channel wise claims reported	To collect information on the claims reported in each state during the quarter.	Quarterly
INPUT_NON_LIFE_CLAIMS_2	Catestrophic/large Claims Details - Statewise	To capture the claims details of catastrophe claims or large claims in each state	Quarterly
INPUT_NONLIFE_Pending_Claims	Claims pending for more than six months and repudiated claims	To capture the details for each instances of claim if pending for more than six months or repudiated	Quarterly

Dept.	Form Name	Dimensions					
		Insurer	LoB	Channel	Geography	Claim Details	Time
Non Life	State wise and channel wise claims reported	X	X		X	X	Q
	Catestrophic/large Claims Details - Statewise	X	X	X	X	X	Q
	Claims pending for more than six months and repudiated claims	X				X	Q


Conceptual Data Model for Non Life Micro Insurance
Insurer
1. Insurer ID
2. Insurer Name
3. Insurer Type
4. Date of Registration
Time
1. Year ID
2. Half Year ID
3. Quarter ID
4. Month ID
5. Day
Non Life Micro Insurance Fact
1. Insurer ID
2. Quarter ID
3. Cover Type ID
4. State ID
Micro Insurance Metrics
Geography
1. Classification
2. Country ID
3. Country Name
4. State ID
5 State Name
6. City Name
7. Pin Code
Cover Type
1. Cover Type ID
2. Cover Type Name

Associated Forms (Non-Life Department- Micro Insurance)			
Code	**Form Name**	**Objective**	**Frequency**
INPUT_NON_LIFE_MI_1	MICROINSURANCE STATISTICS -For the quarter	To gather information on Micro Insurance Business Details across all states.	Quarterly
INPUT_NON_LIFE_MI_1.1	MICROINSURANCE STATISTICS -Upto the quarter	To gather information on Micro Insurance Business Details across all states.	Quarterly

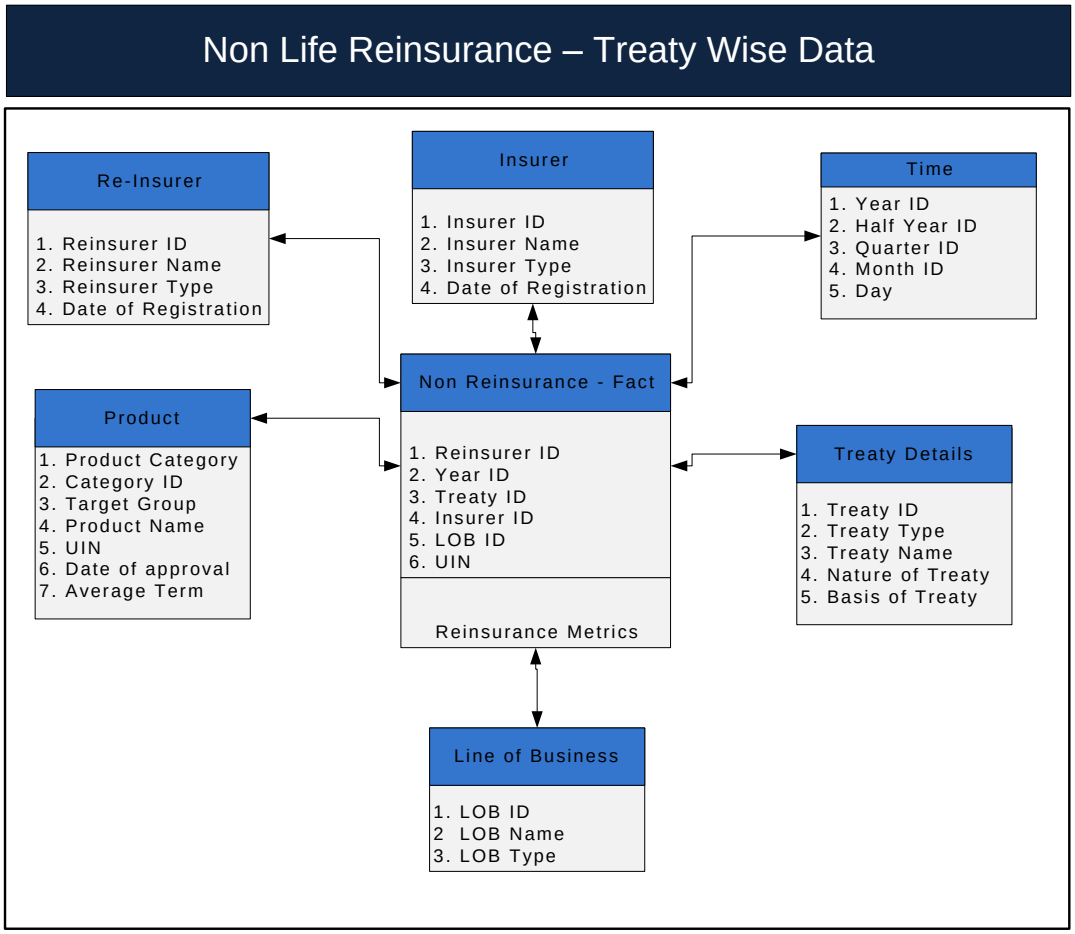
Dept.	Form Name	Dimensions			
		Insurer	Geography	Cover Type	Time
Non Life	MICROINSURANCE STATISTICS -For the quarter	X	X	X	Q
	MICROINSURANCE STATISTICS -Upto the quarter	X	X	X	Q


Non Life – Office Data
Insurer
1. Insurer ID
2. Insurer Name
3. Insurer Type
4. Date of Registration
Time
1. Year ID
2. Half Year ID
3. Quarter ID
4. Month ID
5. Day
Office Data
1. Insurer ID
2. State ID
3. Quarter ID
4. Office ID
5. Location ID
Office Metrics
Office Details
1. Office Type
2. Office ID
3. Office Name
4. Office Address
Geography
1. Classification
2. Country ID
3. Country Name
4. State ID
5 State Name
6. City Name
7. Pin Code
Location
1. Location ID
2. Location Name

Associated Forms (Non Life Department-Office Data)			
Code	**Form Name**	**Objective**	**Frequency**
INPUT_NON_LIFE_Office_1	OFFICE DETAILS-Quarterly	To collect the information on the office (Branch) details in each state for each insurer.	Quarterly
INPUT_NON_LIFE_Office_1.1	Details of foreign offices	To collect the information on the foreign offices classified as representative offices, branches, subsidiaries, agency offices	Quarterly

Dept.	Form Name	Dimensions				
		Insurer	Geography	Office Details	Time	Location
Non Life	OFFICE DETAILS-Quarterly	X	X	X	Q	
	Details of foreign offices	X	X	X	Q	X

3. Non Life Reinsurance Department



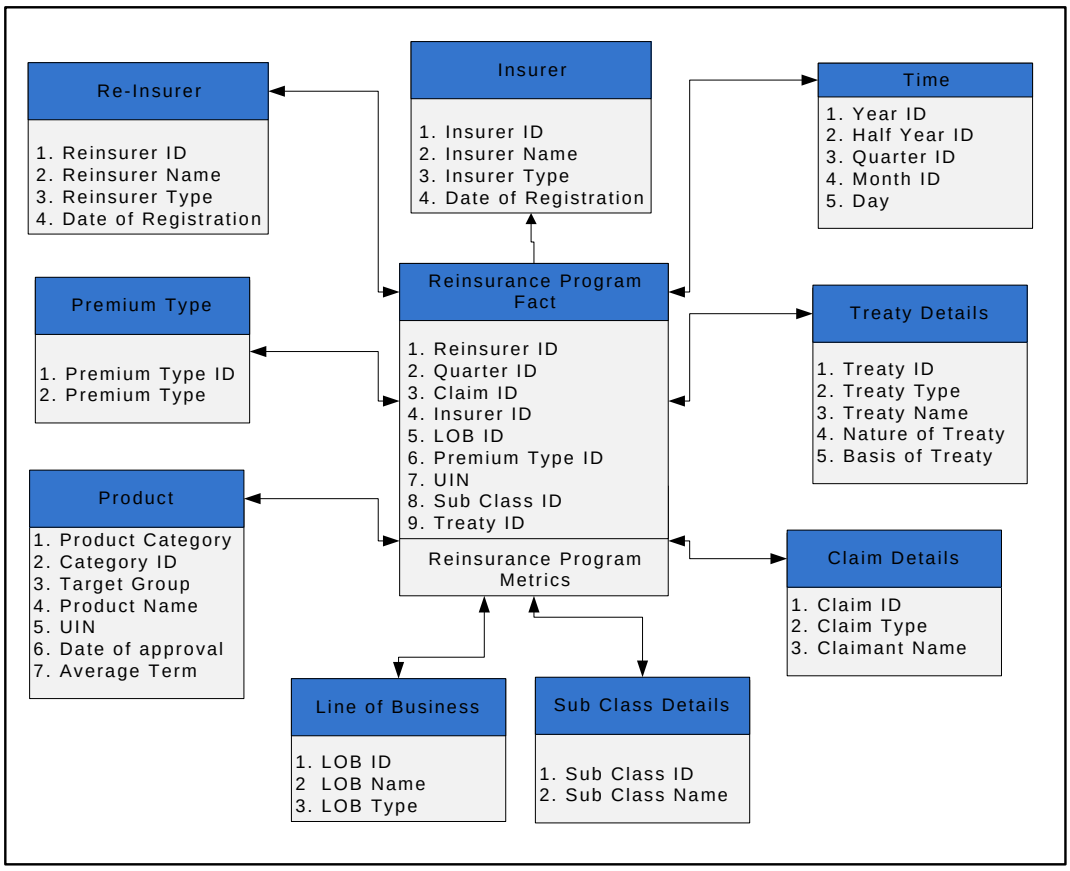
Associated Forms (Non Life Reinsurance Department)			
Code	**Form Name**	**Objective**	**Frequency**
INPUT_NL_REINSURANCE_1	List of reinsurance treaties during the year	To capture the information on the reinsurers, treaties and products covered in each treaty.	Yearly
INPUT_NL_REINSURANCE_1.1	Summary of reinsurance treaties during the year	To capture the summary of the treaties done by the insurers during the year	Yearly
INPUT_NL_REINSURANCE_2	Particulars of Proportional Treaty For the Year	To capture the details of the Proportional treaties filed by the insurer	Yearly
INPUT_NL_REINSURANCE_2.1	Performance of Proportional Treaty - To be furnished by insurers	To collect the performance data on the proportional treaty	Yearly
INPUT_NL_REINSURANCE_3	Particulars of Excess of Loss Cover Treaty For the Year	To capture the details of the excess of loss cover treaties filed by the insurer	Yearly
INPUT_NL_REINSURANCE_3.1	Performance of excess of loss cover treaty - To be furnished by Insurers	To collect the performance data on the Excess of Loss Cover treaty	Yearly
INPUT_NL_REINSURANCE_10	Facultative Placement Compliance Report	To capture the details of the facultative placement data at policy level.	Yearly

Dept.	Form Name	Dimensions					
		Insurer	LoB	Product	Reinsurer	Time	Treaty Details
Non Life Reinsurance	List of reinsurance treaties during the year	X	X	P	X	Y	X
	Summary of reinsurance treaties during the year	X	X			Y	X
	Particulars of Proportional Treaty For the Year	X	X	P	X	Y	X
	Performance of Proportional Treaty - To be furnished by insurers	X			X	Y	X
	Particulars of Excess of Loss Cover Treaty For the Year	X	X	P	X	Y	X
	Performance of excess of loss cover treaty - To be furnished by Insurers	X				Y	X
	Facultative Placement Compliance Report	X	X		X	Y	X

C: Category Level; P: Product level

M: Monthly; Q: Quarterly; Y: Yearly

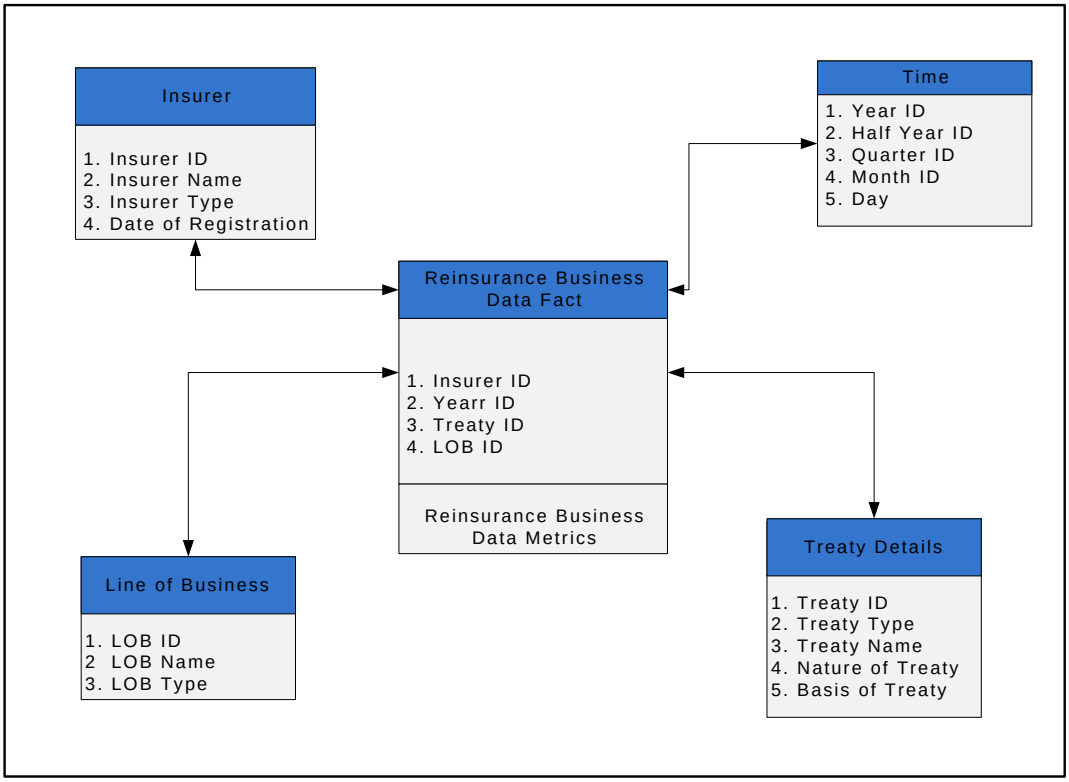
Non Life Reinsurance-Program Data



Associated Forms (Non Life Reinsurance Department)			
Code	**Form Name**	**Objective**	**Frequency**
INPUT_NL_REINSURANCE_1.2	Details of reinsurance Program - To be furnished by Insurer	To collect the details of reinsurance program of each insurer	Yearly
INPUT_NL_REINSURANCE_11	Detailed report on reinsurance program	This report shows of the details of the reinsurance program	Yearly

Dept.	Form Name	Dimensions								
		Insurer	LoB	Product	Reinsurer	Time	Treaty Details	Sub Class	Claim Details	Premium Type
Non Life Reinsurance	Details of reinsurance Program - To be furnished by Insurer	X	X			Y	X	X		X
	Detailed report on reinsurance program	X	X	P	X	Y	X		X	X

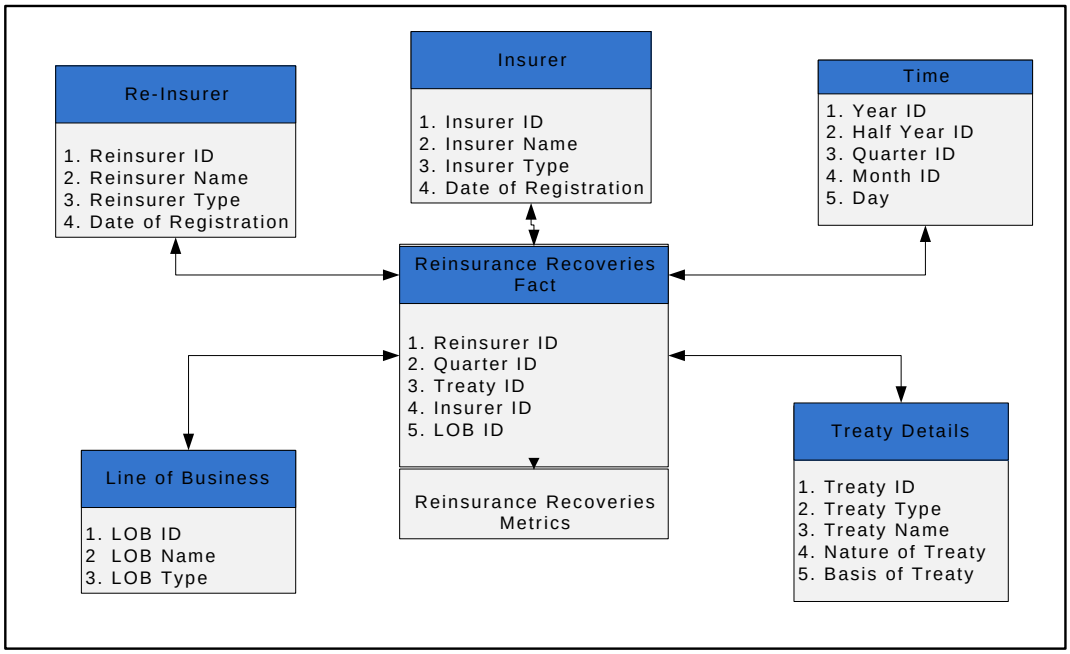
Non Life Reinsurance-Business Data



Associated Forms (Non Life Reinsurance Department)			
Code	**Form Name**	**Objective**	**Frequency**
INPUT_NL_REINSURANCE_4	Reinsurance Statistics under Reg 3(12) - Business Within India (to be furnished by Insurers)	To collect the information on Reinsurance Statistics for Business within India	Yearly
INPUT_NL_REINSURANCE_5	Reinsurance Statistics under Reg 3(12) - Foreign Business (To be furnished by Insurers)	To collect the information on Reinsurance Statistics for Business outside India	Yearly

Dept.	Form Name	Dimensions			
		Insurer	LoB	Time	Treaty Details
Non Life Reinsurance	Reinsurance Statistics under Reg 3(12) - Business Within India (to be furnished by Insurers)	X	X	Y	X
	Reinsurance Statistics under Reg 3(12) - Foreign Business (To be furnished by Insurers)	X	X	Y	X

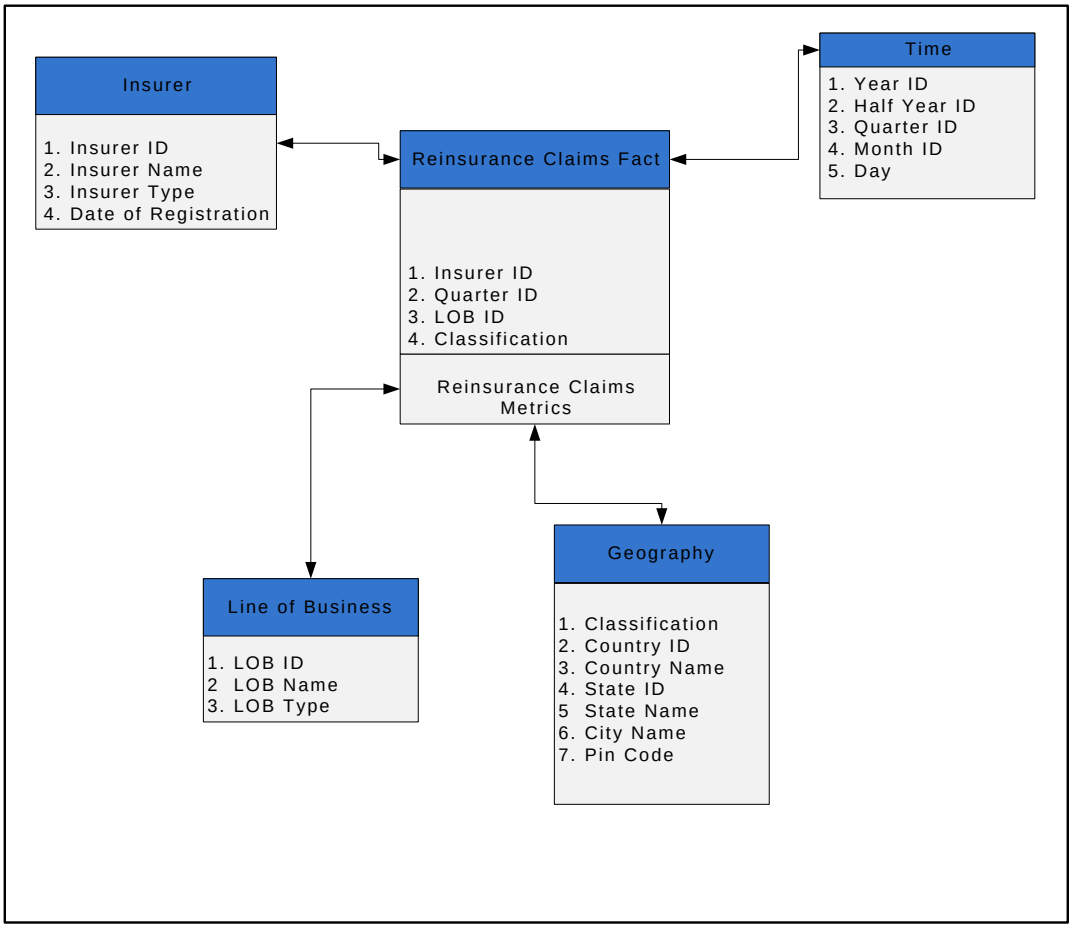
Non Life Reinsurance-Recoveries Data



Associated Forms (Non Life Reinsurance Department)			
Code	**Form Name**	**Objective**	**Frequency**
INPUT_NL_REINSURANCE_6	Details of Outstanding Recoveries - To be furnished by the insurer	To collect information on outstanding recoveries for the reinsurers. This form would be furnished by each insurer	Yearly
INPUT_NL_REINSURANCE_6.1	Aging data of reinsurance recoverable	To capture the details of reinsurance recoverable along with its aging as per different buckets	Quarterly

Dept.	Form Name	Dimensions				
		Insurer	LoB	Time	Treaty Details	Reinsurer
Reinsurance	Details of Outstanding Recoveries - To be furnished by the insurer	X	X	Y	X	X
	Aging data of reinsurance recoverables	X	X	Q	X	X

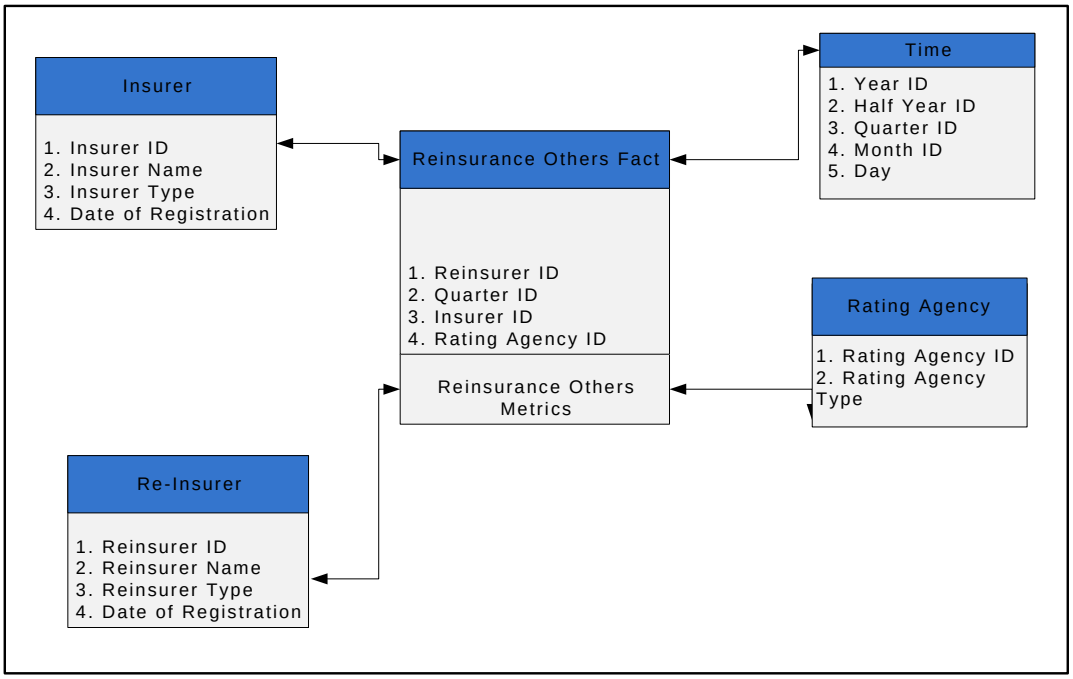
Non Life Reinsurance-Claims Data



Associated Forms (Non Life Reinsurance Department)			
Code	**Form Name**	**Objective**	**Frequency**
INPUT_NL_REINSURANCE_12	Claims data for reinsurance	To capture the claims data related to reinsurance	Quarterly
INPUT_NL_REINSURANCE_13	Premium and Claims Data	To capture the data for premiums and claims with detailed break ups and finally calculating claims ratio	Quarterly

		Insurer	LoB	Time	Geography
Non Life Reinsurance	Claims data for reinsurance	X	X	Q	X
	Premium and Claims Data	X	X	Q	X

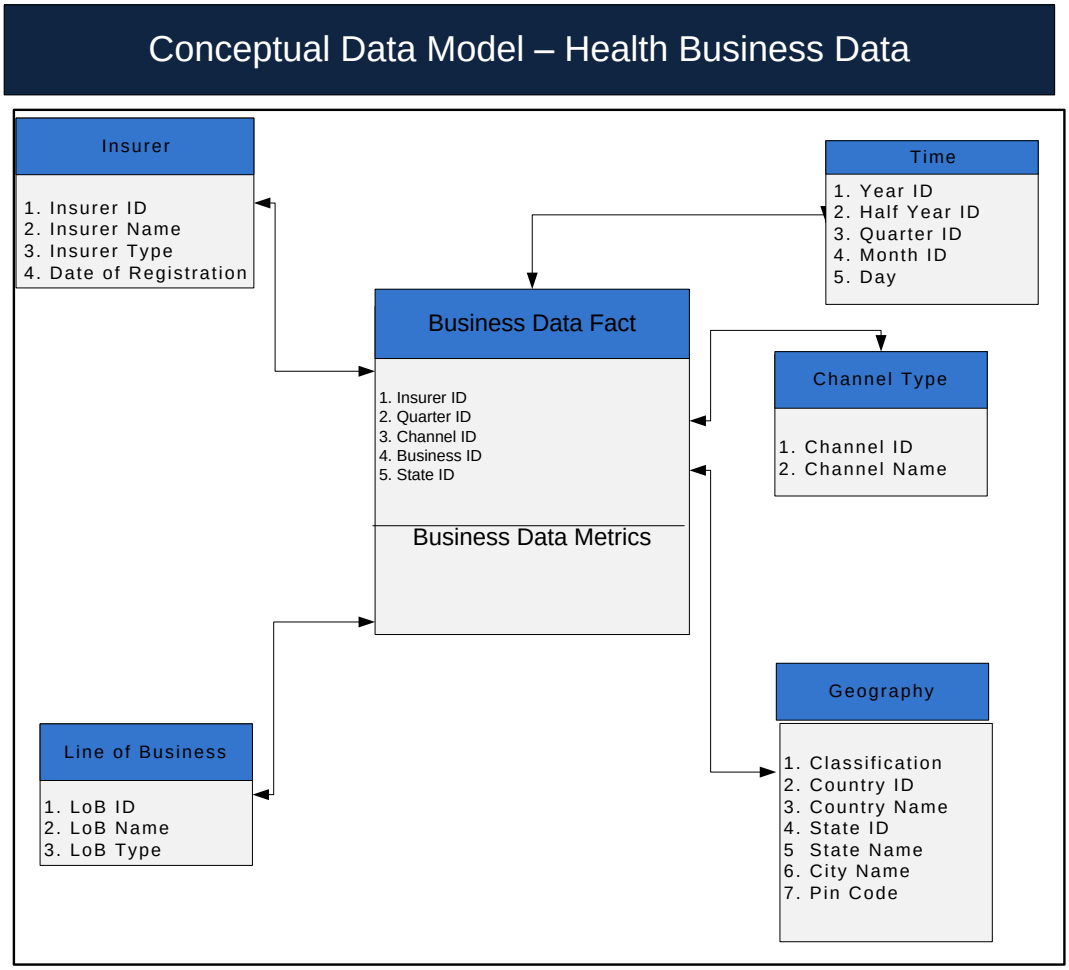
Reinsurance-Others Data



Associated Forms (Reinsurance Department-Others Data)			
Code	**Form Name**	**Objective**	**Frequency**
INPUT_NL_REINSURANCE_9	Reinsurance Concentration	To capture the information on the risk profile of reinsurer in terms of reinsurers' rating.	Yearly

Dept.	Form Name	Dimensions			
		Insurer	Reinsurer	Rating Agency	Time
Reinsurance	Reinsurance Concentration	X	X	X	Y

4. Health Department



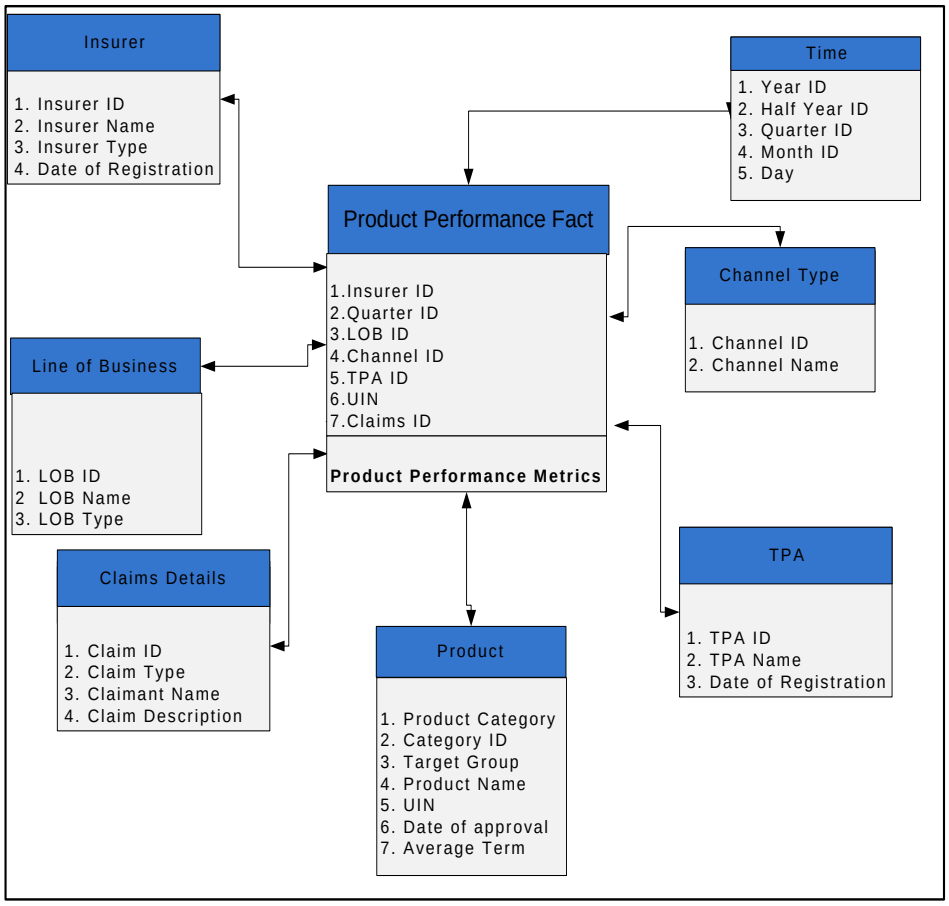
Associated Forms (Health Department)			
Code	**Form Name**	**Objective**	**Frequency**
INPUT_HEALTH_4.1	Details of new business and renewal business - Statewise	To capture the statewise new business and renewal business activities for each insurer	Yearly

Dept.	Form Name	Dimensions				
		Insurer	LoB	Channel	Geography	Time
Health	Details of new business and renewal business - Statewise	X	X	X	X	Q

C: Category Level; P: Product level

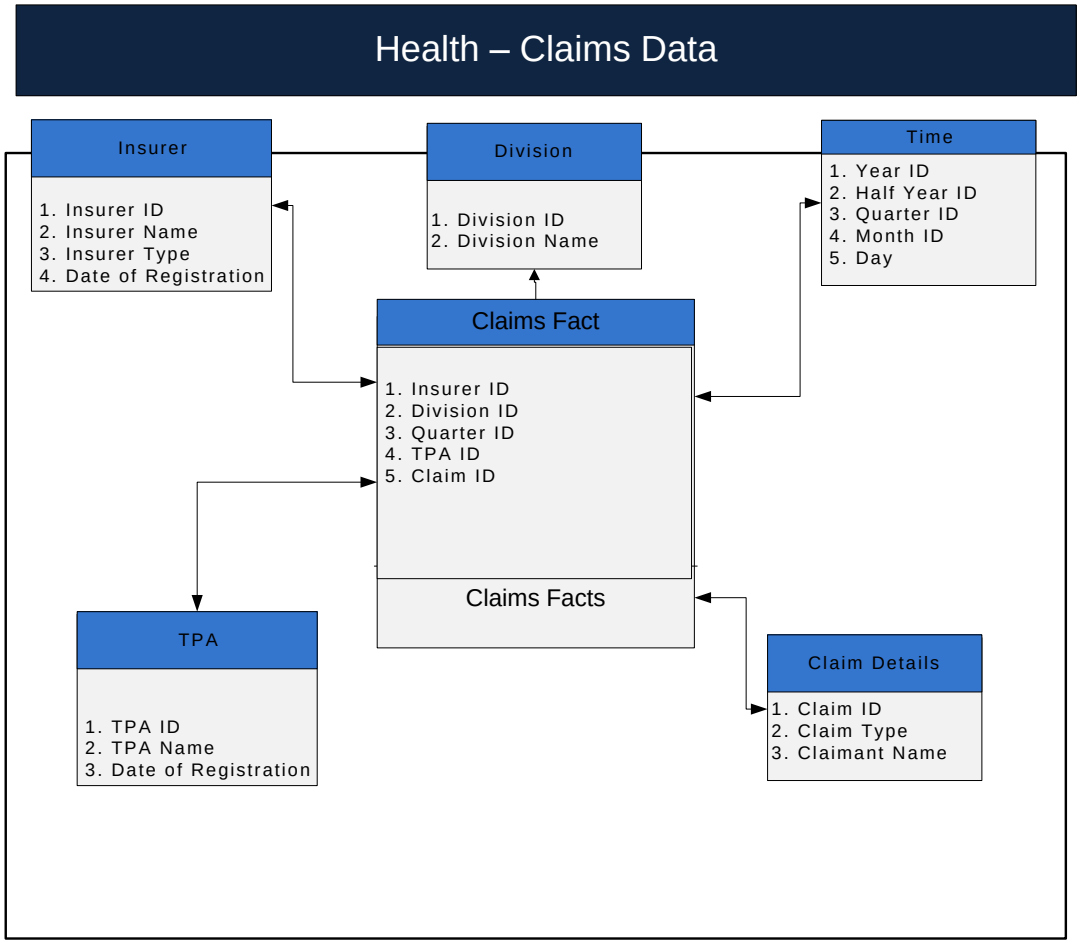
M: Monthly; Q: Quarterly; Y: Yearly

Conceptual Data Model for Health – Product Performance Analysis



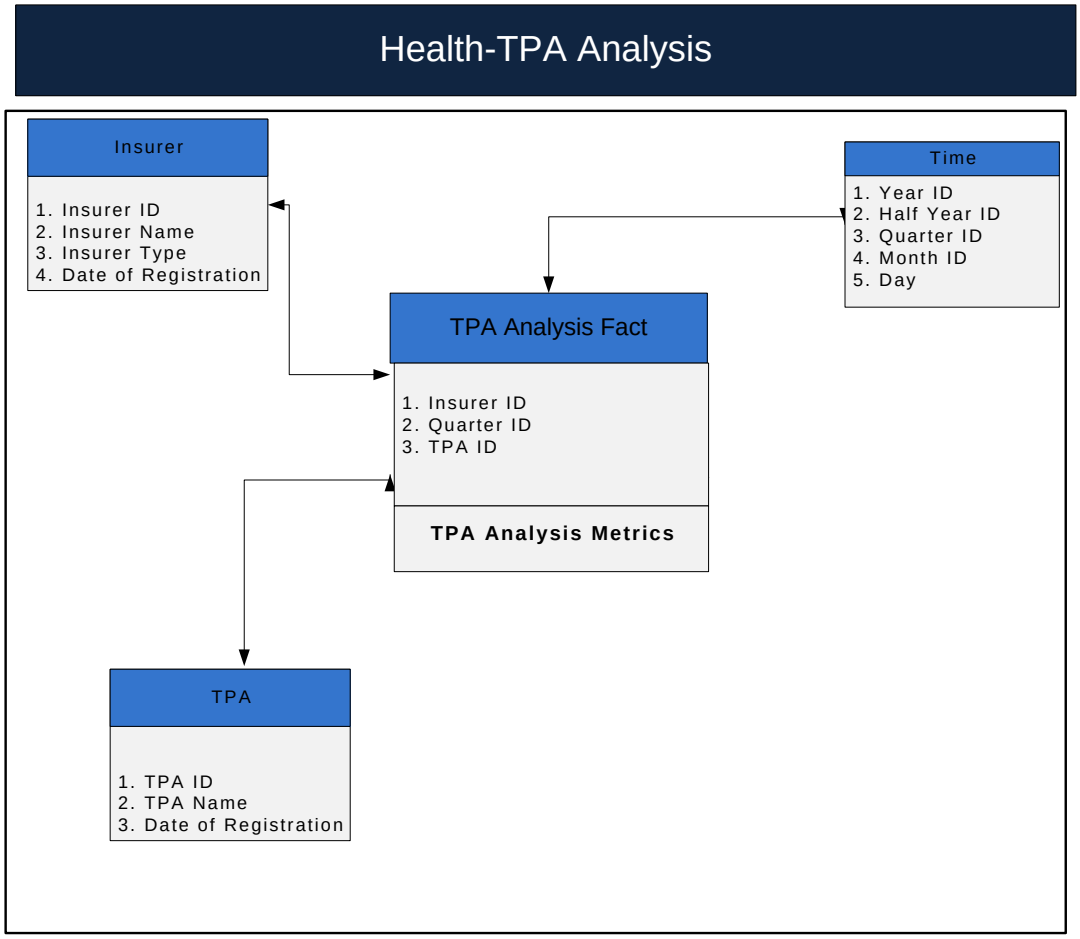
Associated Forms (Health Department)			
Code	**Form Name**	**Objective**	**Frequency**
INPUT_HEALTH_1	Details of product performance - Products with 1 year or less than 1 year term (To be furnished by All insurers having health products)	To collect product information for all products having term 1 year or less than 1 year	Yearly and as and when required
INPUT_HEALTH_1(a)	Details of product performance - Products with more than 1 year term (To be furnished by All insurers having health products)	To collect product information for all products having term more than 1 year	Yearly and as and when required
INPUT_HEALTH_1.1	Details of product performance in terms of claims development and aging (To be furnished by All insurers having health products)	To collect claims movement and claims aging data	Yearly and as and when required
INPUT_HEALTH_2	Details of product performance in terms of claims management w.r.t TPA (To be furnished by insurers having health insurance business)	To capture the performance of the products in terms of claims management w.r.t TPA	Yearly and as and when required
INPUT_HEALTH_3	Details of product performance in terms of channels (To be furnished by insurers having health insurance business)	To capture the performance of the products in terms of distribution channels	Yearly and as and when required
INPUT_HEALTH_6.4	Performance of Universal Health Insurance Scheme (UHIS)/RSBY	This form is used to capture the details of the Performance of Universal Health Insurance Scheme (UHIS)/RSBY for an insurer	Quarterly

Dept.	Form Name	Dimensions						
		Insurer	Product	LoB	Channel	TPA	Claims Type	Time
Health	Details of product performance - Products with 1 year or less than 1 year term (To be furnished by All insurers having health products)	X	P	X				Y
	Details of product performance - Products with more than 1 year term (To be furnished by All insurers having health products)	X	P	X				Y
	Details of product performance in terms of claims development and aging (To be furnished by All insurers having health products)	X	P		X			Y
	Details of product performance in terms of claims management w.r.t TPA (To be furnished by insurers having health insurance business)	X	P			X	X	Y
	Details of product performance in terms of channels (To be furnished by insurers having health insurance business)	X			X			Y
	Performance of Universal Health Insurance Scheme (UHIS)/RSBY	X	P					Q


Health – Claims Data
Insurer
1. Insurer ID
2. Insurer Name
3. Insurer Type
4. Date of Registration
Division
1. Division ID
2. Division Name
Time
1. Year ID
2. Half Year ID
3. Quarter ID
4. Month ID
5. Day
Claims Fact
1. Insurer ID
2. Division ID
3. Quarter ID
4. TPA ID
5. Claim ID
Claims Facts
TPA
1. TPA ID
2. TPA Name
3. Date of Registration
Claim Details
1. Claim ID
2. Claim Type
3. Claimant Name

Associated Forms (Health Department)			
Code	**Form Name**	**Objective**	**Frequency**
INPUT_HEALTH_6	Details of Claims Handled directly- To be submitted by the insurers having health business (Individual)	To collect the information of the claims handled directly by insurers having health business for the individual business	Monthly
INPUT_HEALTH_6.1	Details of Claims Handled directly- To be submitted by the insurers having health business (Group)	To collect the information of the claims handled directly by insurers having health business for the group business	Monthly
INPUT_HEALTH_6.2	Details of Claims Handled through TPA- To be submitted by the insurers having health business	To collect the information of the claims handled through TPA.	Monthly
INPUT_HEALTH_6.3	Details of Claims for an Insurer- Statewise	To collect the information of the claims for an insurer.	Yearly
INPUT_HEALTH_12	Claims Data for TPAs (To be furnished by TPAs)	To capture the claims data for TPAs. And the claims from policyholders, claims from hospitals and claims in aggregate level.	Monthly
INPUT_HEALTH_13	Details of Outstanding Claims (outstanding for more than 6 months) for TPA (To be furnished by TPAs)	To capture the detailed level information about those claims those are outstanding for more than 6 months.	Yearly

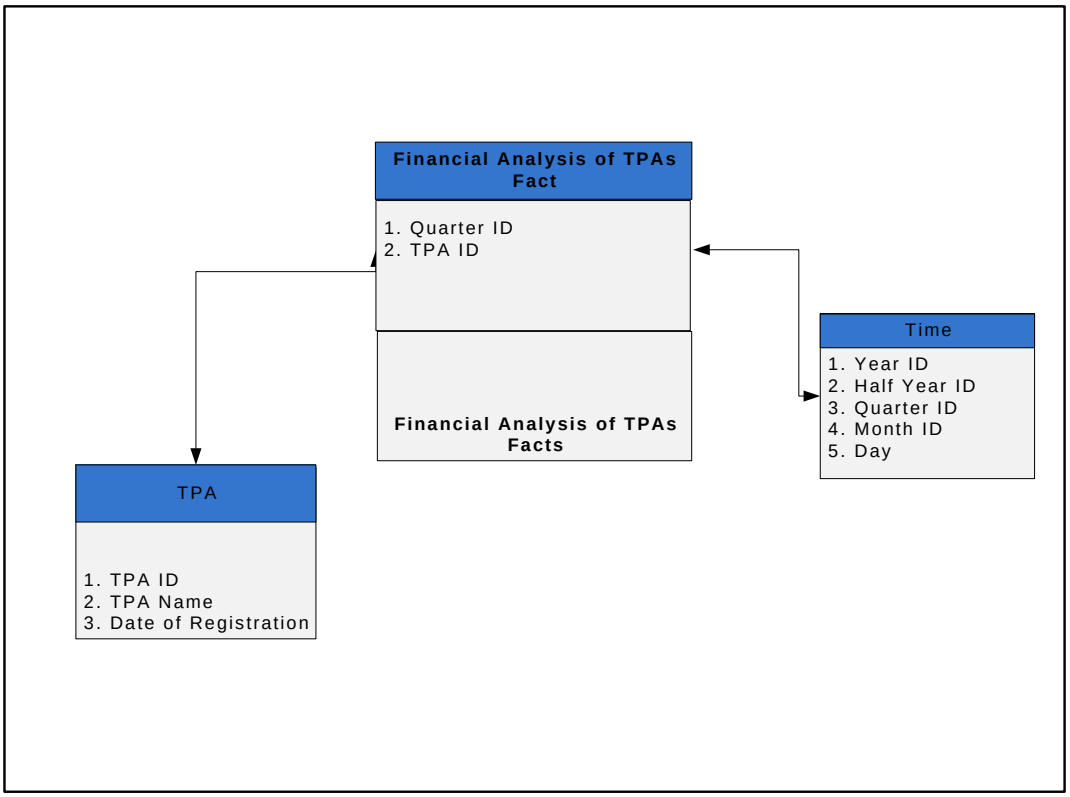
Dept.	Form Name	Dimensions				
		Insurer	Division	Claim Details	TPA	Time
Health	Details of Claims Handled directly- To be submitted by the insurers having health business (Individual)	X		X		M
	Details of Claims Handled directly- To be submitted by the insurers having health business (Group)	X		X		M
	Details of Claims Handled through TPA- To be submitted by the insurers having health business	X	X	X	X	M
	Details of Claims for an Insurer- Statewise	X		X		Y
	Claims Data for TPAs (To be furnished by TPAs)	X		X	X	M
	Details of Outstanding Claims (outstanding for more than 6 months) for TPA (To be furnished by TPAs)			X	X	Y


Health-TPA Analysis
Insurer
1. Insurer ID
2. Insurer Name
3. Insurer Type
4. Date of Registration
Time
1. Year ID
2. Half Year ID
3. Quarter ID
4. Month ID
5. Day
TPA Analysis Fact
1. Insurer ID
2. Quarter ID
3. TPA ID
TPA Analysis Metrics
TPA
1. TPA ID
2. TPA Name
3. Date of Registration

Associated Forms (Health Department)			
Code	**Form Name**	**Objective**	**Frequency**
INPUT_HEALTH_5	Details of Due payable to TPA	To measure the effectiveness of functions of TPAs in terms of claim float and TPA Fees	Monthly
INPUT_HEALTH_7	Details of TPA Administrative Configuration (To be furnished by TPAs)	To capture the existing administrative configuration of TPA. This form includes data on directors, CEOs and CAOs.	Yearly
INPUT_HEALTH_8	TPA Contract Details (To be furnished by TPAs)	To capture the data on the contracts of TPAs with insurers and hospitals/doctors along with the data on claims processed during previous year	Yearly

Dept.	Form Name	Dimensions		
		Insurer	TPA	Time
Health	Details of Due payable to TPA	X	X	M
	Details of TPA Administrative Configuration (To be furnished by TPAs)		X	Y
	TPA Contract Details (To be furnished by TPAs)	X	X	Y

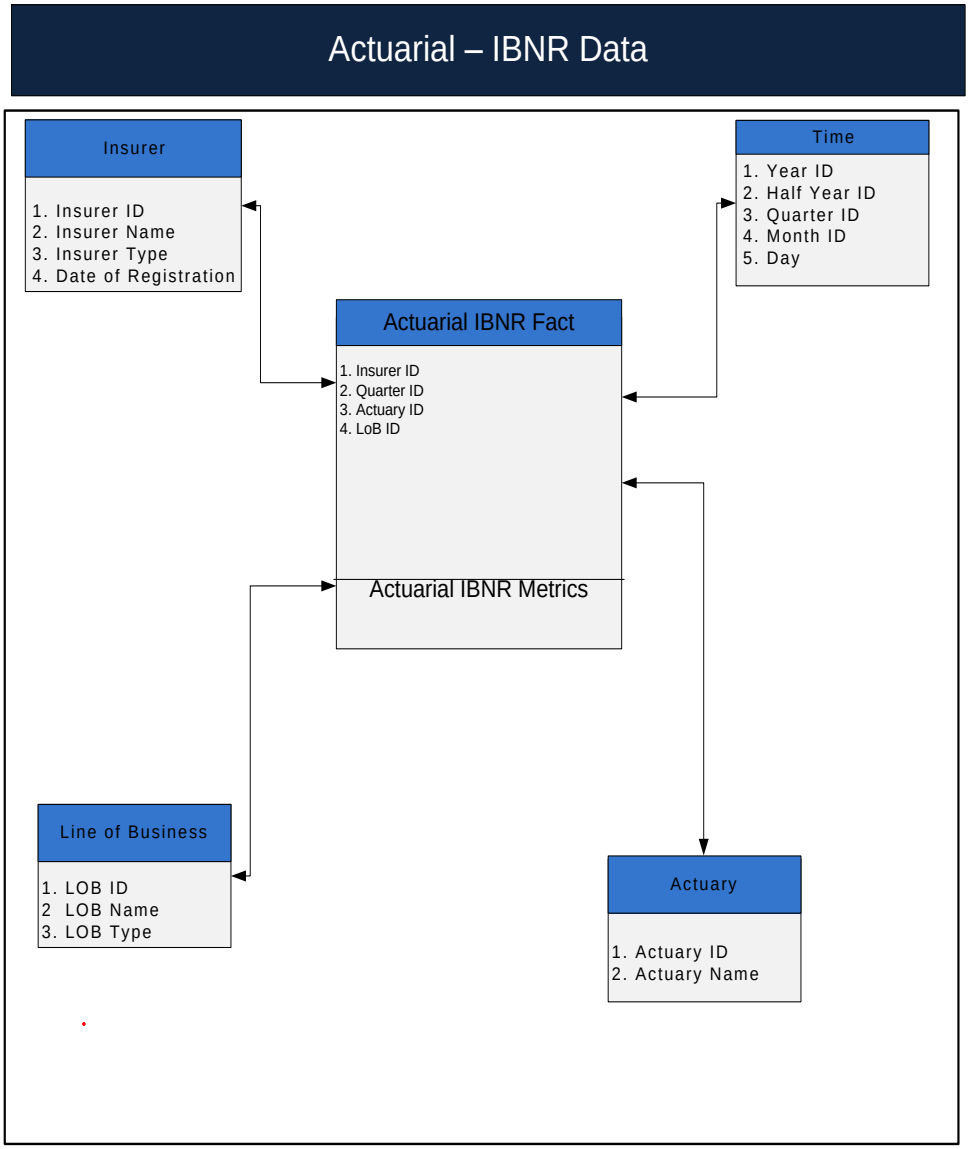
Health –TPA Financial Analysis



Associated Forms (Health Department)			
Code	**Form Name**	**Objective**	**Frequency**
INPUT_HEALTH_8.1	Contract Details and Share Holding pattern (To be furnished by TPAs) - Quarterly	To collect data on details of capital structure and shareholding pattern of TPAs.	Quarterly
INPUT_HEALTH_9	Profit & Loss Statement for TPAs (To be furnished by TPAs)	This return contains the Profit & Loss Statement of the TPAs. The format of profit and loss statement is standard across all TPAs for easy consolidation of the financials	Yearly
INPUT_HEALTH_10	Profit & Loss Appropriation Format for TPAs (To be furnished by TPAs)	To capture the profit & loss appropriation for each TPA	Yearly
INPUT_HEALTH_11	Balance Sheet for TPAs (To be furnished by TPAs)	To represent the balance sheet items of the TPAs.	Yearly

Dept.	Form Name	Dimensions	
		TPA	Time
Health	Contract Details and Share Holding pattern (To be furnished by TPAs) - Quarterly	X	Q
	Profit & Loss Statement for TPAs (To be furnished by TPAs)	X	Y
	Profit & Loss Appropriation Format for TPAs (To be furnished by TPAs)	X	Y
	Balance Sheet for TPAs (To be furnished by TPAs)	X	Y

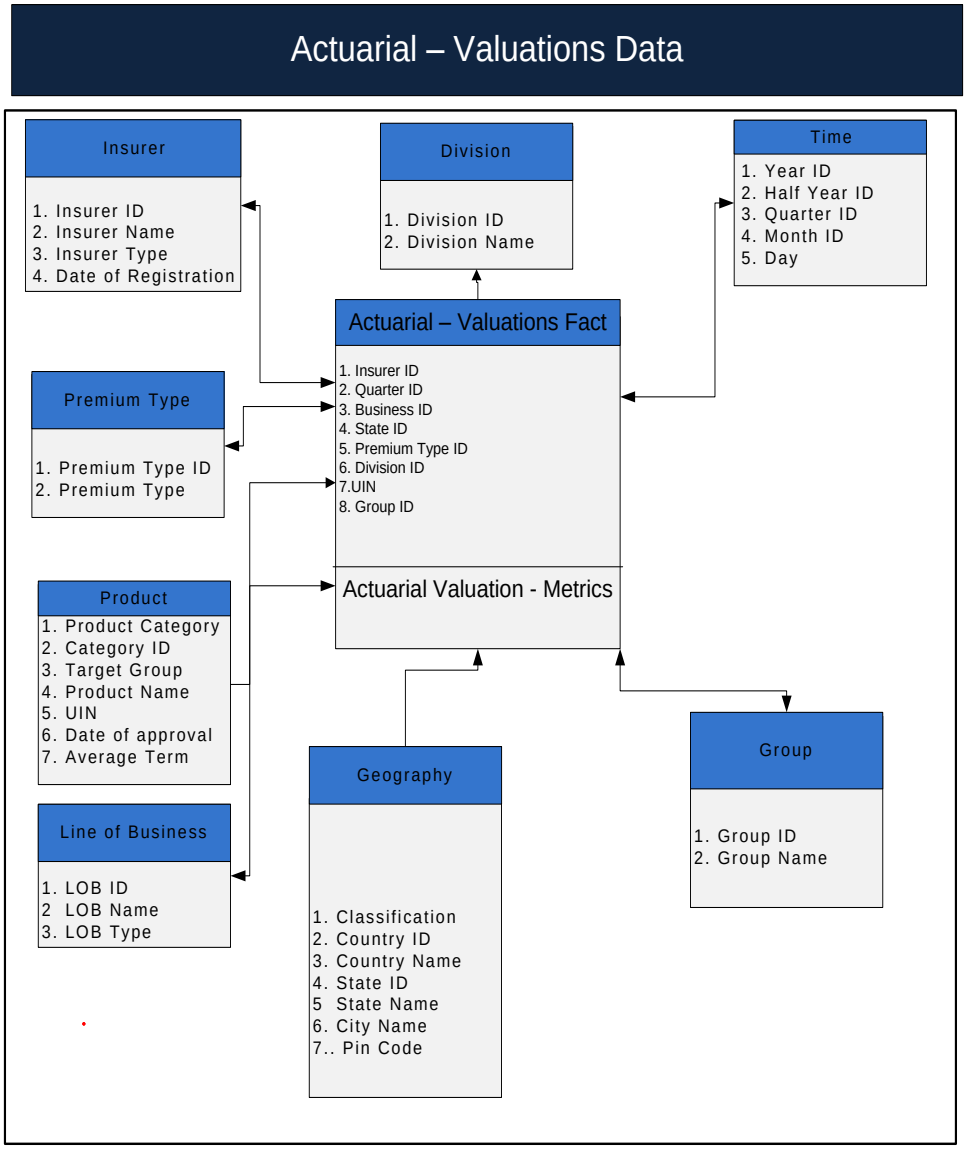
5. Actuarial Department



Associated Forms (Actuarial Department)			
Code	**Form Name**	**Objective**	**Frequency**
INPUT_NL_ACTUARIAL_1	IBNR-A: Statement of IBNR Provision	To capture data on IBNR Provisions for those policies	Quarterly
INPUT_NL_ACTUARIAL_2	IBNR-B1(a):Cumulative Statement of Paid Claims Development (By Amount)	To capture data on amount of paid claims development in terms of amount	Quarterly
INPUT_NL_ACTUARIAL_2.1	IBNR-B1(b):Cumulative Statement of Incurred Claims Development (By Amount)	To capture data on amount of incurred claims development in terms of amount	Quarterly
INPUT_NL_ACTUARIAL_3	IBNR-B2(a):Cumulative Statement of Paid Claims Development (By Number)	To capture data on incurred claims development in terms of number	Quarterly
INPUT_NL_ACTUARIAL_3.1	IBNR-B2(b):Cumulative Statement of Incurred Claims Development (By Number)	To capture data on incurred claims development in terms of number	Quarterly
INPUT_NL_ACTUARIAL_4	Utilization of Claims Data - Accident Year Wise	To capture the utilization of claims data - accident year wise	Quarterly

Associated Forms (Actuarial Department)			
Code	**Form Name**	**Objective**	**Frequency**
INPUT_NL_ACTUARIAL_5	Utilization of Claims Data - Financial Year Wise	To capture the utilization of claims data – financial year wise	Quarterly
INPUT_NL_ACTUARIAL_6	Incurred Claims Ratio Data - Accident Year Wise	To capture incurred claims ratio data - Accident year wise	Quarterly

		Insurer	Actuary	LoB	Time
Actuarial	IBNR-A: Statement of IBNR Provision	X	X	X	Q
	IBNR-B1(a):Cumulative Statement of Paid Claims Development (By Amount)	X	X	X	Q
	IBNR-B1(b):Cumulative Statement of Incurred Claims Development (By Amount)	X	X	X	Q
	IBNR-B2(a):Cumulative Statement of Paid Claims Development (By Number)	X	X	X	Q
	IBNR-B2(b):Cumulative Statement of Incurred Claims Development (By Number)	X	X	X	Q
	Utilization of Claims Data - Accident Year Wise	X			Q
	Utilization of Claims Data - Financial Year Wise	X			Y
	Incurred Claims Ratio Data - Accident Year Wise	X			Y


Actuarial – Valuations Data
Insurer
1. Insurer ID
2. Insurer Name
3. Insurer Type
4. Date of Registration
Division
1. Division ID
2. Division Name
Time
1. Year ID
2. Half Year ID
3. Quarter ID
4. Month ID
5. Day
Actuarial – Valuations Fact
1. Insurer ID
2. Quarter ID
3. Business ID
4. State ID
5. Premium Type ID
6. Division ID
7.UIN
8. Group ID
Actuarial Valuation - Metrics
Premium Type
1. Premium Type ID
2. Premium Type
Product
1. Product Category
2. Category ID
3. Target Group
4. Product Name
5. UIN
6. Date of approval
7. Average Term
Line of Business
1. LOB ID
2 LOB Name
3. LOB Type
Geography
1. Classification
2. Country ID
3. Country Name
4. State ID
5 State Name
6. City Name
7.. Pin Code
Group
1. Group ID
2. Group Name

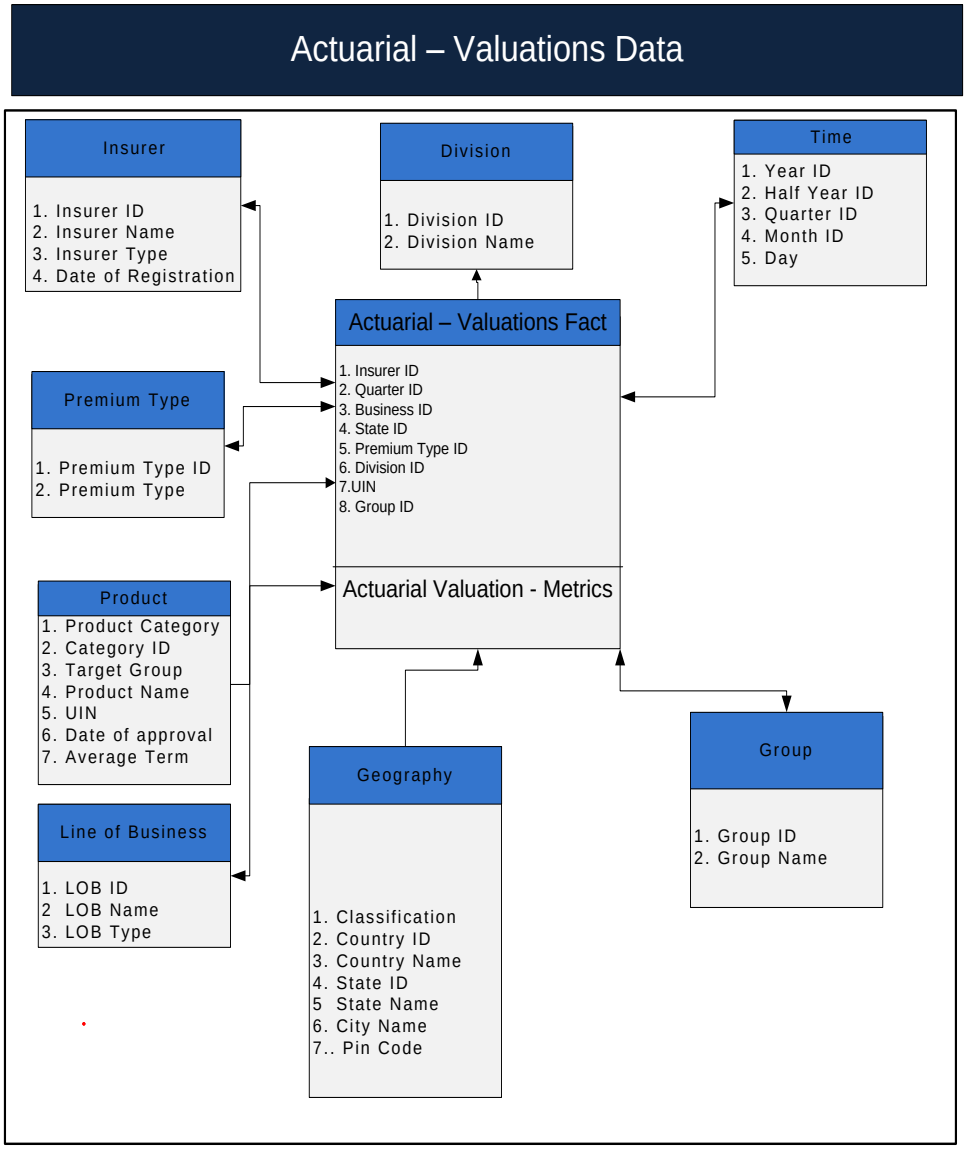
Associated Forms (Actuarial Department)			
Code	**Form Name**	**Objective**	**Frequency**
INPUT_ACTUARIAL_1	Form DD - Form for New Business and Total In-Force Business Data	To capture the data on new business in the year and total in-force business during the year.	Yearly
INPUT_ACTUARIAL_2	Form DDD - Form for Business Movement during the year	To capture the business movement during the year	Yearly
INPUT_ACTUARIAL_3	Form DDDD - Details of Lapsed and Reinstated policies	To capture the details of lapsed policies and reinstated policies during the year	Yearly
INPUT_ACTUARIAL_4	Form NLB 1 - Details of in-force policies at product level (Non-Linked Policies)	To capture the details of in-force policies at product level in the year	Yearly
INPUT_ACTUARIAL_5	Form LB 1 - Details of in-force policies at product level (Linked Business)	To capture the details of in-force policies at product level in the year	Yearly
INPUT_ACTUARIAL_6	Form LB 2 - Statement of Net Asset Value for the Segregated	To capture the performance of the segregated funds in unit linked business in the year	Yearly

Associated Forms (Actuarial Department)			
Code	**Form Name**	**Objective**	**Frequency**
	Funds Maintained by the insurer (Linked Business)		
INPUT_ACTUARIAL_7	Form LB 3 - Statement of No. of units in the Segregated Funds Maintained by the insurer (Linked Business)	To capture the data of units of the segregated funds in unit linked business in the year	Yearly
INPUT_ACTUARIAL_8	Form KT-1 - Statement of solvency margin	To capture the data on solvency margin maintained by insurer in the year	Yearly
INPUT_ACTUARIAL_9	Form KT-2 - Statement of solvency margin	To capture the data on solvency margin maintained by insurer in the year	Yearly
INPUT_ACTUARIAL_10	Form KT - Q - Statement of available solvency margin and solvency ratio	To capture the data on solvency margin maintained by insurer in the quarter	Quarterly
INPUT_ACTUARIAL_10.1	Form KT - 3 - Statement of available solvency margin and solvency ratio	To capture the data on solvency margin maintained by insurer in the year	Yearly

Associated Forms (Actuarial Department)			
Code	**Form Name**	**Objective**	**Frequency**
INPUT_ACTUARIAL_11	Form IA	To capture the information on negative reserves	Yearly
INPUT_ACTUARIAL_12	Form H	To capture the mathematical reserves at classification and category level.	Yearly
INPUT_ACTUARIAL_13	Valuation Bases	To capture the valuation parameters used in the valuation of products	Yearly
INPUT_ACTUARIAL_14	Return on Assets	To capture the details of return on assets for policyholders' fund and shareholders' fund	Yearly
INPUT_ACTUARIAL_15	Details of foreign operation	To capture the details of the foreign operations of each insurer	Yearly
INPUT_ACTUARIAL_16	Components of global reserves	To capture the details of additional information on global reserves	Yearly

		Insurer	Product	LoB	Premium Type	Division	Geography	Group	Time
Actuarial	Form DD - Form for New Business and Total In-Force Business Data	X	C	X	X	X	X	X	Y
	Form DDD - Form for Business Movement during the year	X	C	X	X	X	X	X	Y
	Form DDDD - Details of Lapsed and Reinstated policies	X	C	X	X	X	X	X	Y
	Form NLB 1 - Details of in-force policies at	X	P	X	X	X	X	X	Y

		Insurer	Product	LoB	Premium Type	Division	Geography	Group	Time
	product level (Non-Linked Policies)								
	Form LB 1 - Details of in-force policies at product level (Linked Business)	X	C		X		X		Y
	Form LB 2 - Statement of Net Asset Value for the Segregated Funds Maintained by the insurer (Linked Business)	X	C	X	X	X	X	X	Y
	Form LB 3 - Statement of No. of units in the Segregated Funds Maintained by the insurer (Linked Business)	X	P	X	X	X	X	X	Y
	Form KT-1 - Statement of solvency margin	X	C			X	X		Y
	Form KT-2 - Statement of solvency margin	X					X		Y
	Form KT - Q - Statement of available solvency margin and solvency ratio	X					X		Q
	Form KT - 3 - Statement of available solvency margin and solvency ratio	X					X		Y
	Form IA	X	C				X	X	Y
	Form H	X	C	X		X	X	X	Y
	Valuation Bases	X	P		X				Y
	Return on Assets	X							Y
	Details of foreign operation	X					X		Y
	Components of global reserves	X							Y


Actuarial – Valuations Data
Insurer
1. Insurer ID
2. Insurer Name
3. Insurer Type
4. Date of Registration
Division
1. Division ID
2. Division Name
Time
1. Year ID
2. Half Year ID
3. Quarter ID
4. Month ID
5. Day
Actuarial – Valuations Fact
1. Insurer ID
2. Quarter ID
3. Business ID
4. State ID
5. Premium Type ID
6. Division ID
7.UIN
8. Group ID
Premium Type
1. Premium Type ID
2. Premium Type
Actuarial Valuation - Metrics
Product
1. Product Category
2. Category ID
3. Target Group
4. Product Name
5. UIN
6. Date of approval
7. Average Term
Line of Business
1. LOB ID
2 LOB Name
3. LOB Type
Geography
1. Classification
2. Country ID
3. Country Name
4. State ID
5 State Name
6. City Name
7.. Pin Code
Group
1. Group ID
2. Group Name

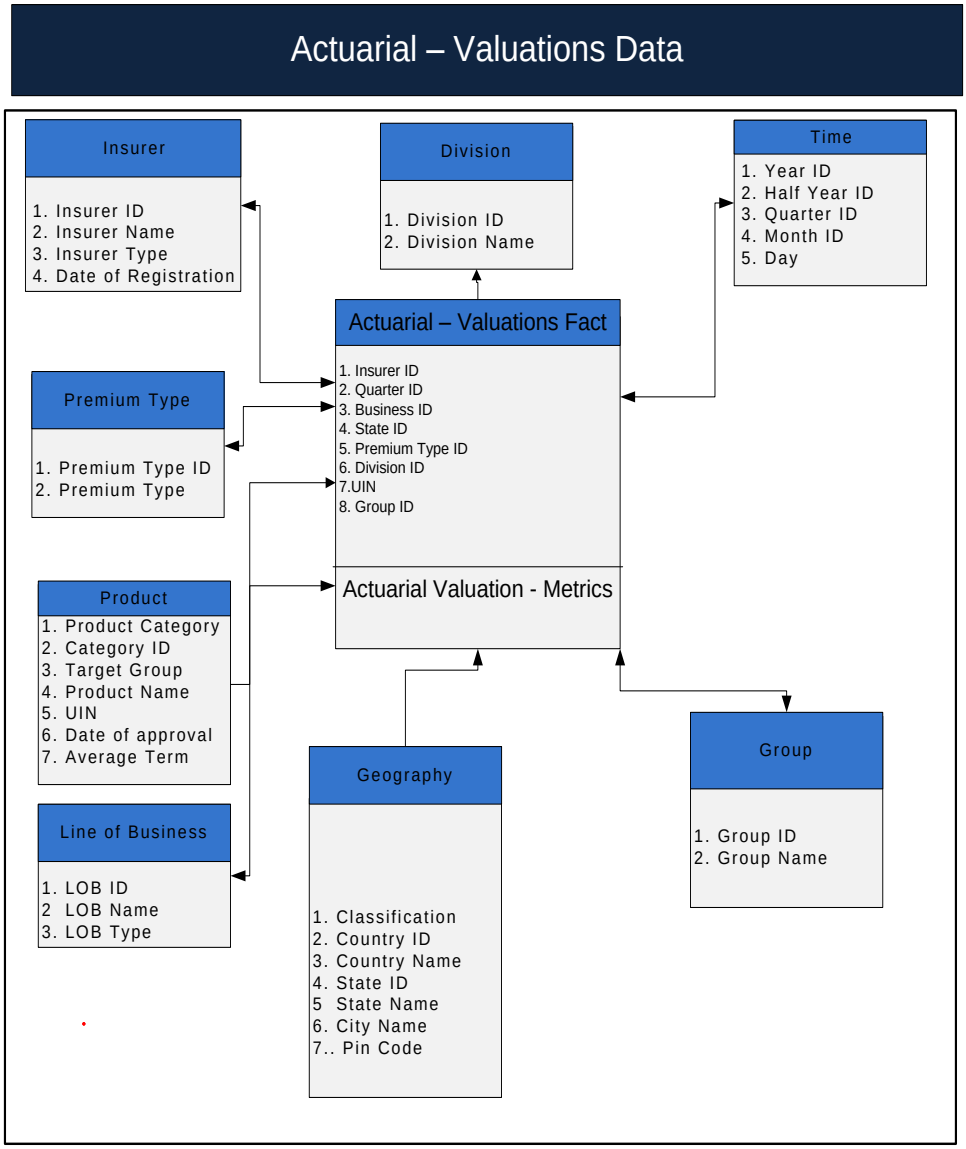
Associated Forms (Actuarial Department)			
Code	**Form Name**	**Objective**	**Frequency**
INPUT_ACTUARIAL_1	Form DD - Form for New Business and Total In-Force Business Data	To capture the data on new business in the year and total in-force business during the year.	Yearly
INPUT_ACTUARIAL_2	Form DDD - Form for Business Movement during the year	To capture the business movement during the year	Yearly
INPUT_ACTUARIAL_3	Form DDDD - Details of Lapsed and Reinstated policies	To capture the details of lapsed policies and reinstated policies during the year	Yearly
INPUT_ACTUARIAL_4	Form NLB 1 - Details of in-force policies at product level (Non-Linked Policies)	To capture the details of in-force policies at product level in the year	Yearly
INPUT_ACTUARIAL_5	Form LB 1 - Details of in-force policies at product level (Linked Business)	To capture the details of in-force policies at product level in the year	Yearly
INPUT_ACTUARIAL_6	Form LB 2 - Statement of Net Asset Value for the Segregated	To capture the performance of the segregated funds in unit linked business in the year	Yearly

Associated Forms (Actuarial Department)			
Code	**Form Name**	**Objective**	**Frequency**
	Funds Maintained by the insurer (Linked Business)		
INPUT_ACTUARIAL_7	Form LB 3 - Statement of No. of units in the Segregated Funds Maintained by the insurer (Linked Business)	To capture the data of units of the segregated funds in unit linked business in the year	Yearly
INPUT_ACTUARIAL_8	Form KT-1 - Statement of solvency margin	To capture the data on solvency margin maintained by insurer in the year	Yearly
INPUT_ACTUARIAL_9	Form KT-2 - Statement of solvency margin	To capture the data on solvency margin maintained by insurer in the year	Yearly
INPUT_ACTUARIAL_10	Form KT - Q - Statement of available solvency margin and solvency ratio	To capture the data on solvency margin maintained by insurer in the quarter	Quarterly
INPUT_ACTUARIAL_10.1	Form KT - 3 - Statement of available solvency margin and solvency ratio	To capture the data on solvency margin maintained by insurer in the year	Yearly

Associated Forms (Actuarial Department)			
Code	**Form Name**	**Objective**	**Frequency**
INPUT_ACTUARIAL_11	Form IA	To captures the information on negative reserves	Yearly
INPUT_ACTUARIAL_12	Form H	To capture the mathematical reserves at classification and category level.	Yearly
INPUT_ACTUARIAL_13	Valuation Bases	To capture the valuation parameters used in the valuation of products	Yearly
INPUT_ACTUARIAL_14	Return on Assets	To capture the details of return on assets for policyholders' fund and shareholders' fund	Yearly
INPUT_ACTUARIAL_15	Details of foreign operation	To capture the details of the foreign operations of each insurer	Yearly
INPUT_ACTUARIAL_16	Components of global reserves	To capture the details of additional information on global reserves	Yearly

		Insurer	Product	LoB	Premium Type	Division	Geography	Group	Time
Actuarial	Form DD - Form for New Business and Total In-Force Business Data	X	C	X	X	X	X	X	Y
	Form DDD - Form for Business Movement during the year	X	C	X	X	X	X	X	Y
	Form DDDD - Details of Lapsed and Reinstated policies	X	C	X	X	X	X	X	Y
	Form NLB 1 - Details of in-force policies at	X	P	X	X	X	X	X	Y

		Insurer	Product	LoB	Premium Type	Division	Geography	Group	Time
	product level (Non-Linked Policies)								
	Form LB 1 - Details of in-force policies at product level (Linked Business)	X	C		X		X		Y
	Form LB 2 - Statement of Net Asset Value for the Segregated Funds Maintained by the insurer (Linked Business)	X	C	X	X	X	X	X	Y
	Form LB 3 - Statement of No. of units in the Segregated Funds Maintained by the insurer (Linked Business)	X	P	X	X	X	X	X	Y
	Form KT-1 - Statement of solvency margin	X	C			X	X		Y
	Form KT-2 - Statement of solvency margin	X					X		Y
	Form KT - Q - Statement of available solvency margin and solvency ratio	X					X		Q
	Form KT - 3 - Statement of available solvency margin and solvency ratio	X					X		Y
	Form IA	X	C				X	X	Y
	Form H	X	C	X		X	X	X	Y
	Valuation Bases	X	P		X				Y
	Return on Assets	X							Y
	Details of foreign operation	X					X		Y
	Components of global reserves	X							Y


Actuarial – Valuations Data
Insurer
1. Insurer ID
2. Insurer Name
3. Insurer Type
4. Date of Registration
Division
1. Division ID
2. Division Name
Time
1. Year ID
2. Half Year ID
3. Quarter ID
4. Month ID
5. Day
Actuarial – Valuations Fact
1. Insurer ID
2. Quarter ID
3. Business ID
4. State ID
5. Premium Type ID
6. Division ID
7.UIN
8. Group ID
Premium Type
1. Premium Type ID
2. Premium Type
Actuarial Valuation - Metrics
Product
1. Product Category
2. Category ID
3. Target Group
4. Product Name
5. UIN
6. Date of approval
7. Average Term
Line of Business
1. LOB ID
2 LOB Name
3. LOB Type
Geography
1. Classification
2. Country ID
3. Country Name
4. State ID
5 State Name
6. City Name
7.. Pin Code
Group
1. Group ID
2. Group Name

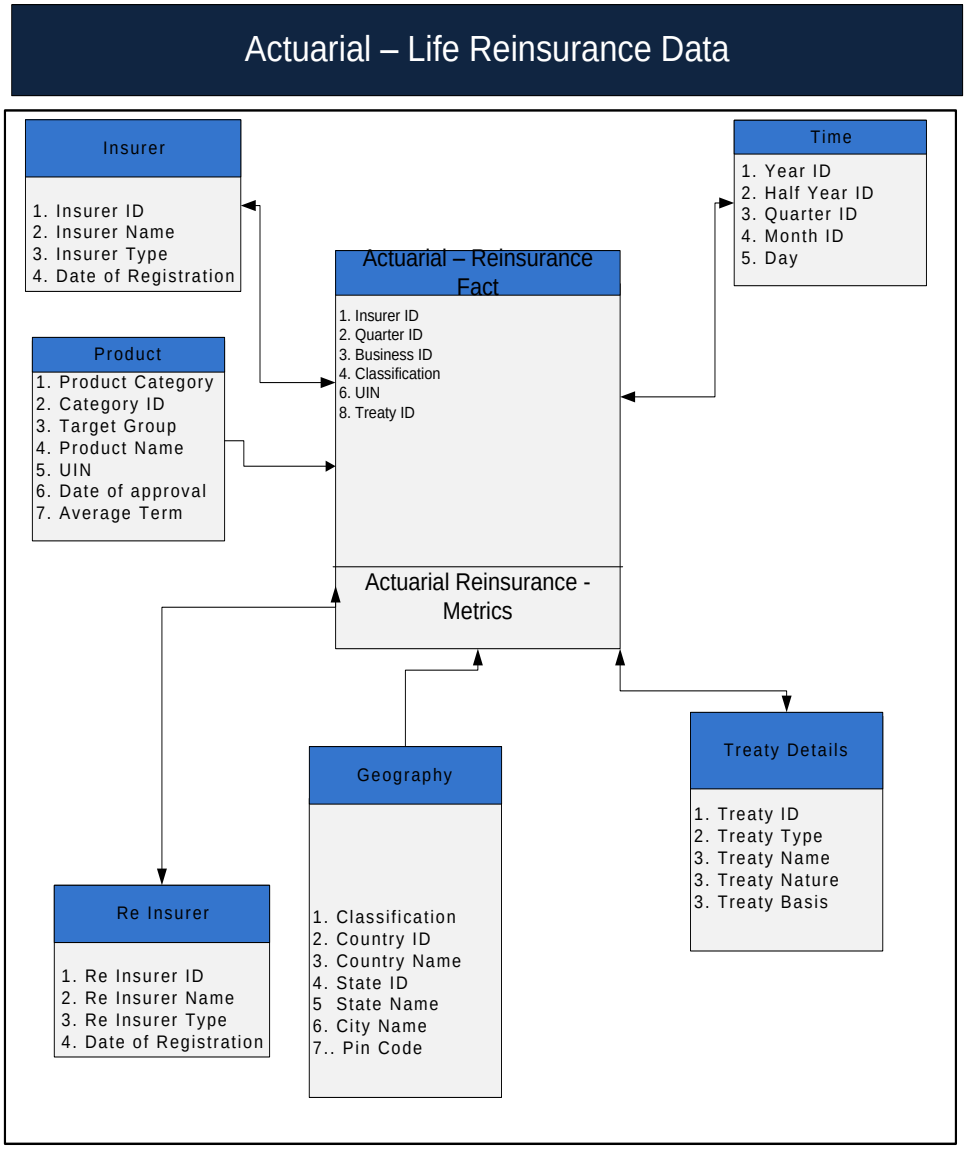
Associated Forms (Actuarial Department)			
Code	**Form Name**	**Objective**	**Frequency**
INPUT_ACTUARIAL_1	Form DD - Form for New Business and Total In-Force Business Data	To capture the data on new business in the year and total in-force business during the year.	Yearly
INPUT_ACTUARIAL_2	Form DDD - Form for Business Movement during the year	To capture the business movement during the year	Yearly
INPUT_ACTUARIAL_3	Form DDDD - Details of Lapsed and Reinstated policies	To capture the details of lapsed policies and reinstated policies during the year	Yearly
INPUT_ACTUARIAL_4	Form NLB 1 - Details of in-force policies at product level (Non-Linked Policies)	To capture the details of in-force policies at product level in the year	Yearly
INPUT_ACTUARIAL_5	Form LB 1 - Details of in-force policies at product level (Linked Business)	To capture the details of in-force policies at product level in the year	Yearly
INPUT_ACTUARIAL_6	Form LB 2 - Statement of Net Asset Value for the Segregated	To capture the performance of the segregated funds in unit linked business in the year	Yearly

Associated Forms (Actuarial Department)			
Code	**Form Name**	**Objective**	**Frequency**
	Funds Maintained by the insurer (Linked Business)		
INPUT_ACTUARIAL_7	Form LB 3 - Statement of No. of units in the Segregated Funds Maintained by the insurer (Linked Business)	To capture the data of units of the segregated funds in unit linked business in the year	Yearly
INPUT_ACTUARIAL_8	Form KT-1 - Statement of solvency margin	To capture the data on solvency margin maintained by insurer in the year	Yearly
INPUT_ACTUARIAL_9	Form KT-2 - Statement of solvency margin	To capture the data on solvency margin maintained by insurer in the year	Yearly
INPUT_ACTUARIAL_10	Form KT - Q - Statement of available solvency margin and solvency ratio	To capture the data on solvency margin maintained by insurer in the quarter	Quarterly
INPUT_ACTUARIAL_10.1	Form KT - 3 - Statement of available solvency margin and solvency ratio	To capture the data on solvency margin maintained by insurer in the year	Yearly

Associated Forms (Actuarial Department)			
Code	**Form Name**	**Objective**	**Frequency**
INPUT_ACTUARIAL_11	Form IA	To captures the information on negative reserves	Yearly
INPUT_ACTUARIAL_12	Form H	To capture the mathematical reserves at classification and category level.	Yearly
INPUT_ACTUARIAL_13	Valuation Bases	To capture the valuation parameters used in the valuation of products	Yearly
INPUT_ACTUARIAL_14	Return on Assets	To capture the details of return on assets for policyholders' fund and shareholders' fund	Yearly
INPUT_ACTUARIAL_15	Details of foreign operation	To capture the details of the foreign operations of each insurer	Yearly
INPUT_ACTUARIAL_16	Components of global reserves	To capture the details of additional information on global reserves	Yearly

		Insurer	Product	LoB	Premium Type	Division	Geography	Group	Time
Actuarial	Form DD - Form for New Business and Total In-Force Business Data	X	C	X	X	X	X	X	Y
	Form DDD - Form for Business Movement during the year	X	C	X	X	X	X	X	Y
	Form DDDD - Details of Lapsed and Reinstated policies	X	C	X	X	X	X	X	Y
	Form NLB 1 - Details of in-force policies at	X	P	X	X	X	X	X	Y

		Insurer	Product	LoB	Premium Type	Division	Geography	Group	Time
	product level (Non-Linked Policies)								
	Form LB 1 - Details of in-force policies at product level (Linked Business)	X	C		X		X		Y
	Form LB 2 - Statement of Net Asset Value for the Segregated Funds Maintained by the insurer (Linked Business)	X	C	X	X	X	X	X	Y
	Form LB 3 - Statement of No. of units in the Segregated Funds Maintained by the insurer (Linked Business)	X	P	X	X	X	X	X	Y
	Form KT-1 - Statement of solvency margin	X	C			X	X		Y
	Form KT-2 - Statement of solvency margin	X					X		Y
	Form KT - Q - Statement of available solvency margin and solvency ratio	X					X		Q
	Form KT - 3 - Statement of available solvency margin and solvency ratio	X					X		Y
	Form IA	X	C				X	X	Y
	Form H	X	C	X		X	X	X	Y
	Valuation Bases	X	P		X				Y
	Return on Assets	X							Y
	Details of foreign operation	X					X		Y
	Components of global reserves	X							Y

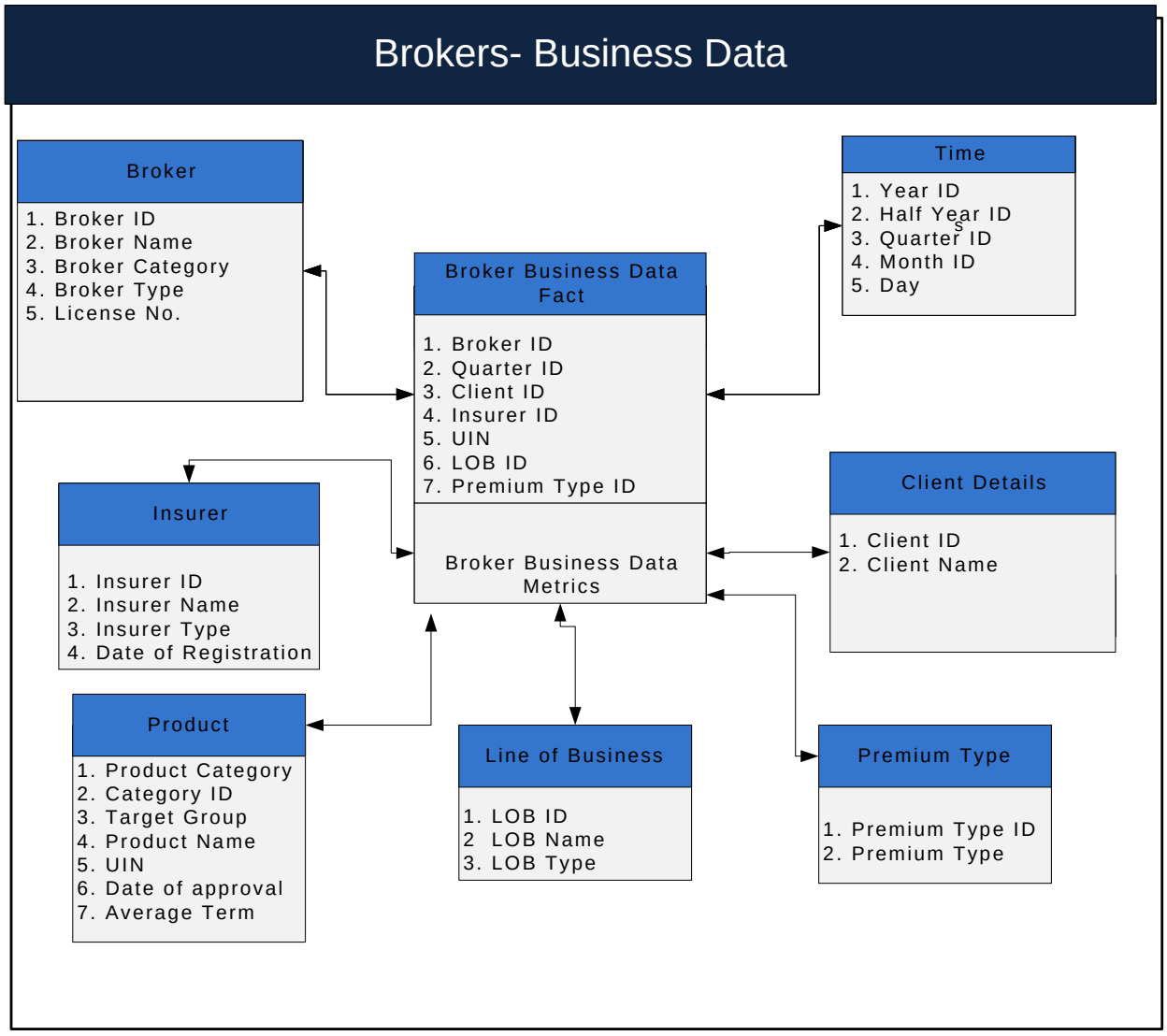

Actuarial – Life Reinsurance Data
Insurer
1. Insurer ID
2. Insurer Name
3. Insurer Type
4. Date of Registration
Time
1. Year ID
2. Half Year ID
3. Quarter ID
4. Month ID
5. Day
Actuarial – Reinsurance Fact
1. Insurer ID
2. Quarter ID
3. Business ID
4. Classification
6. UIN
8. Treaty ID
Product
1. Product Category
2. Category ID
3. Target Group
4. Product Name
5. UIN
6. Date of approval
7. Average Term
Actuarial Reinsurance - Metrics
Treaty Details
1. Treaty ID
2. Treaty Type
3. Treaty Name
3. Treaty Nature
3. Treaty Basis
Geography
1. Classification
2. Country ID
3. Country Name
4. State ID
5 State Name
6. City Name
7.. Pin Code
Re Insurer
1. Re Insurer ID
2. Re Insurer Name
3. Re Insurer Type
4. Date of Registration

Associated Forms (Actuarial Department)			
Code	**Form Name**	**Objective**	**Frequency**
INPUT_REINSURANCE_1	Form LR-1: List of reinsurance treaties for the year	To capture the information on the reinsurers, treaties and products covered in each treaty.	Yearly
INPUT_REINSURANCE_1.1	Summary of reinsurance treaties during the year	To capture the summary of the treaties done by the insurers during the year	Yearly
INPUT_REINSURANCE_2	Form LR-2: Particulars of Surplus Treaty For the Year	To capture the details of the surplus treaties filed by the insurer	Yearly
INPUT_REINSURANCE_1	Form LR-3: Result of Surplus Treaty	To capture the business data of the reinsurance for surplus treaty	Yearly
INPUT_REINSURANCE_4	Form LR-4: Particulars of Quota Share Treaty For the Year	To capture the details of the quota share treaties filed by the insurer	Yearly
INPUT_REINSURANCE_5	Form LR-5: Result of Quota Share surplus Treaty for	To collect the business data of the reinsurance for quota share surplus treaty	Yearly
INPUT_REINSURANCE_6	Form LR-6: Particulars of Excess of Loss cover/Catastrophe Treaty For the Year	To capture the details of the excess of loss/catastrophe treaties filed by the insurer	Yearly
INPUT_REINSURANCE_7	Form LR-7: Result of Excess of Loss/catastrophe Treaty	To capture the business data of the reinsurance for Excess of Loss/catastrophe Treaty	Yearly

Associated Forms (Actuarial Department)			
Code	**Form Name**	**Objective**	**Frequency**
INPUT_REINSURANCE_8	Form LR-8: Reinsurance Accounts for the quarter	To capture the business data of the reinsurance for all treaties	Quarterly

		Insurer	Product	Reinsurer	Treaty	Geography	Time
Actuarial	Form LR-1: List of reinsurance treaties for the year	X	P	X	X	X	Y
	Summary of reinsurance treaties during the year	X	C			X	Y
	Form LR-2: Particulars of Surplus Treaty For the Year	X	P	X	X	X	Y
	Form LR-3: Result of Surplus Treaty	X	C	X	X	X	Y
	Form LR-4: Particulars of Quota Share Treaty For the Year	X	P	X	X	X	Y
	Form LR-5: Result of Quota Share surplus Treaty for	X	C	X	X	X	Y
	Form LR-6: Particulars of Excess of Loss cover/Catastrophe Treaty For the Year	X	P	X	X	X	Y
	Form LR-7: Result of Excess of Loss/catastrophe Treaty	X	C	X	X	X	Y
	Form LR-8: Reinsurance Accounts for the quarter	X	C			X	Q

6. Intermediaries – Brokers Department



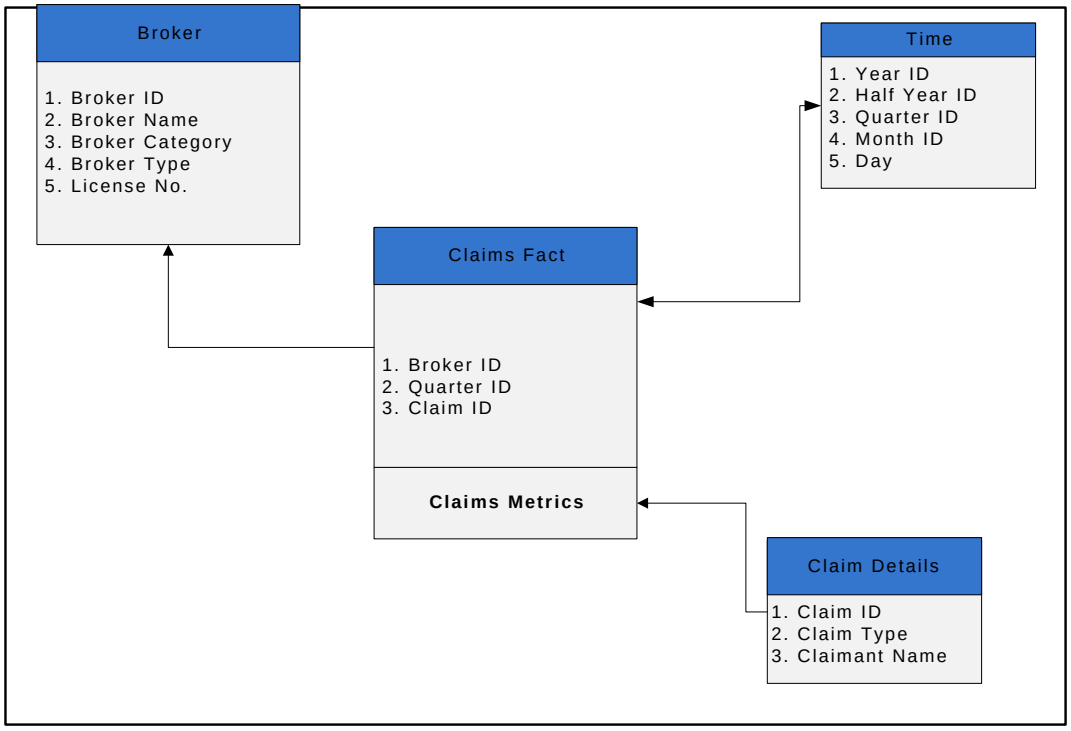
Associated Forms (Brokers Department)			
Code	**Form Name**	**Objective**	**Frequency**
INPUT_BROKER_10	Business Data for brokers	To capture the new business data for a broker insurer wise and client wise	Yearly
INPUT_BROKER_10.1	Business Data for brokers (Life Insurers)	To capture the new business data for brokers for life insurers	Quarterly
INPUT_BROKER_10.2	Business Data for brokers (Non Life Insurers)	To capture the new business data for brokers for non life insurers	Quarterly

Dept.	Form Name	Dimensions						
		Broker	Insurer	Time	Client	Premium Type	Product Category	LoB
Brokers	Business Data for brokers	X	X	Y	X			
	Business Data for brokers (Life Insurers)	X		Q		X	P	X
	Business Data for brokers (Non Life Insurers)	X		Q				X

C: Category Level; P: Product level

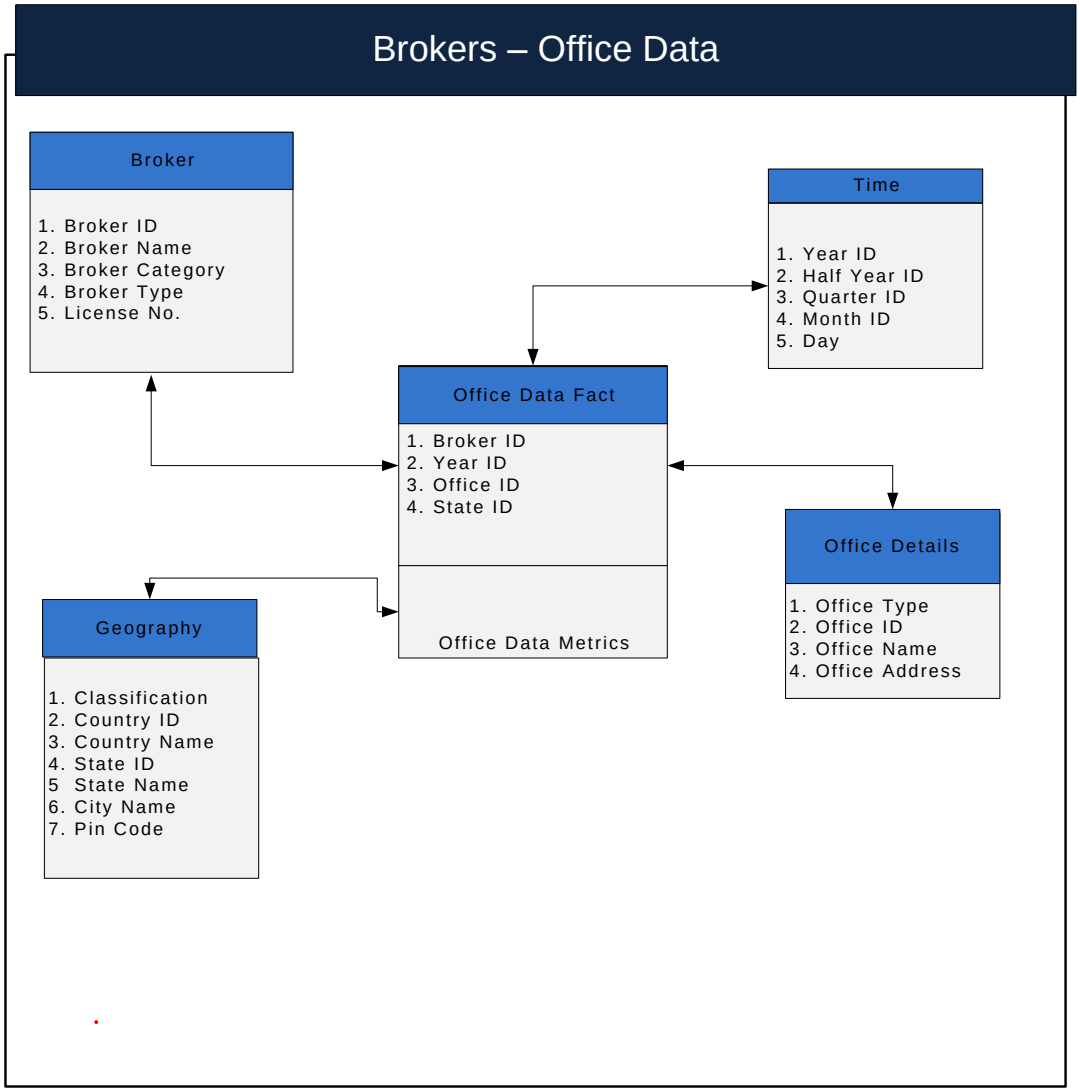
M: Monthly; Q: Quarterly; Y: Yearly

Broker – Claims Data



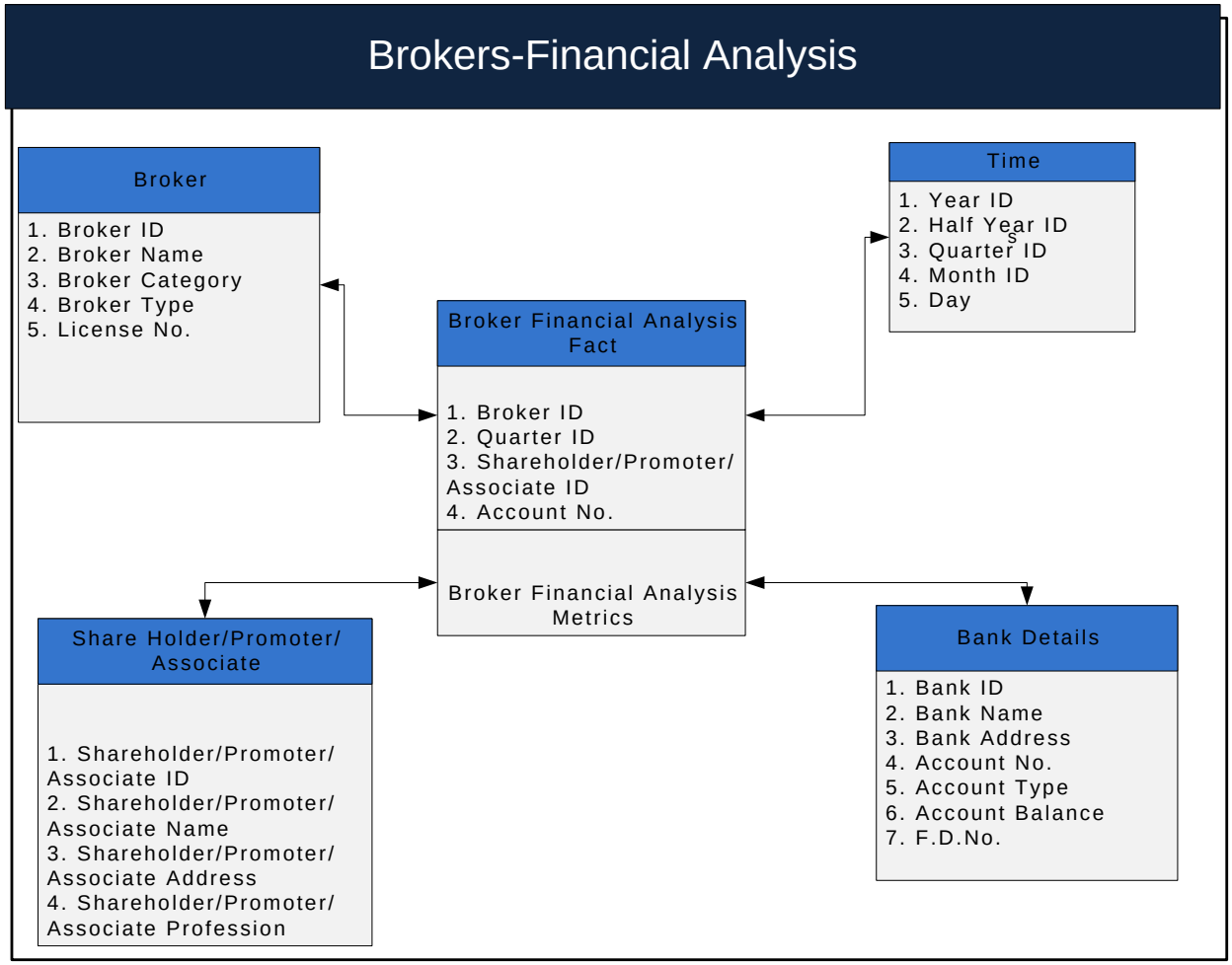
Associated Forms (Brokers Department- Claims Data)			
Code	**Form Name**	**Objective**	**Frequency**
INPUT_BROKER_12	Claims Data	To capture the details of the claims for a broker	Quarterly

Dept.	Form Name	Dimensions		
		Broker	Claim Details	Time
Brokers	Claims Data	X	X	Q


Brokers – Office Data
Broker
1. Broker ID
2. Broker Name
3. Broker Category
4. Broker Type
5. License No.
Time
1. Year ID
2. Half Year ID
3. Quarter ID
4. Month ID
5. Day
Office Data Fact
1. Broker ID
2. Year ID
3. Office ID
4. State ID
Office Data Metrics
Office Details
1. Office Type
2. Office ID
3. Office Name
4. Office Address
Geography
1. Classification
2. Country ID
3. Country Name
4. State ID
5 State Name
6. City Name
7. Pin Code

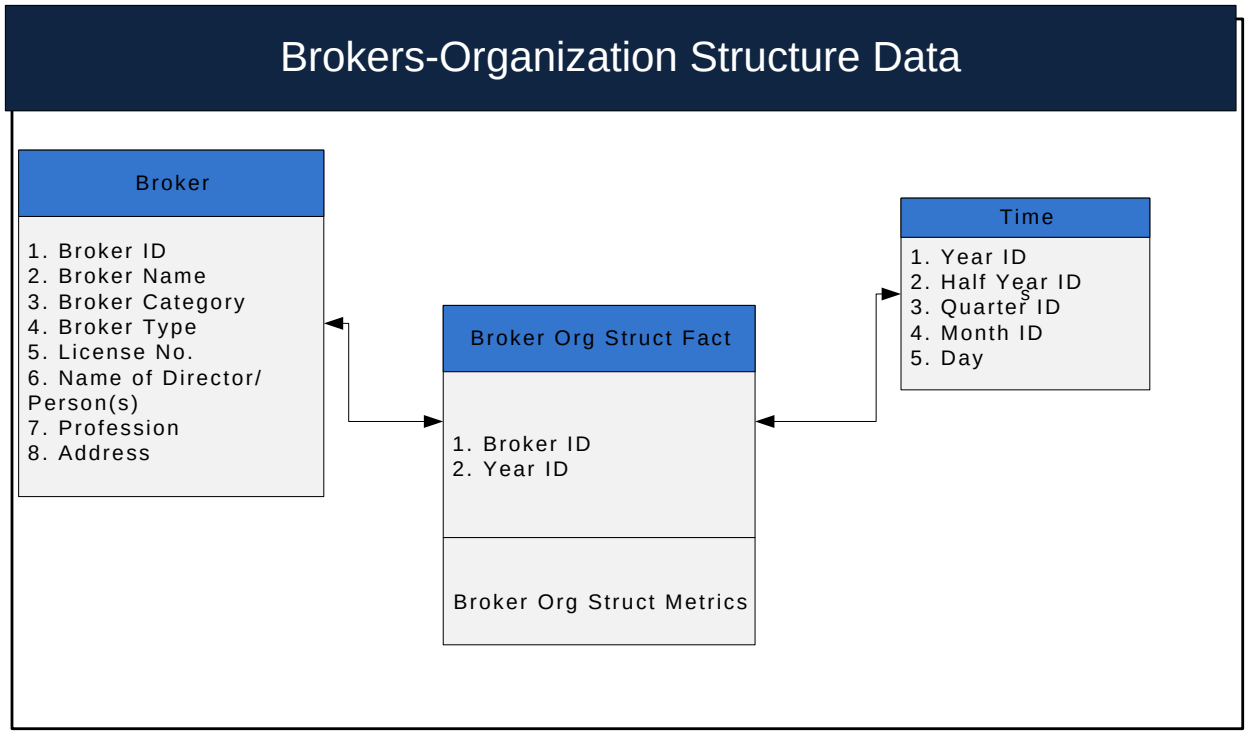
Associated Forms (Brokers Department)			
Code	**Form Name**	**Objective**	**Frequency**
INPUT_BROKER_2	Particular of branch and registered offices	To capture the details of a branch office for a broker	Yearly

Dept.	Form Name	Dimensions			
		Broker	Geography	Office	Time
Brokers	Particular of branch and registered offices	X	X	X	Y


Brokers-Financial Analysis
Broker
1. Broker ID
2. Broker Name
3. Broker Category
4. Broker Type
5. License No.
Time
1. Year ID
2. Half Year ID
3. Quarter ID
4. Month ID
5. Day
Broker Financial Analysis Fact
1. Broker ID
2. Quarter ID
3. Shareholder/Promoter/ Associate ID
4. Account No.
Broker Financial Analysis Metrics
Share Holder/Promoter/ Associate
1. Shareholder/Promoter/ Associate ID
2. Shareholder/Promoter/ Associate Name
3. Shareholder/Promoter/ Associate Address
4. Shareholder/Promoter/ Associate Profession
Bank Details
1. Bank ID
2. Bank Name
3. Bank Address
4. Account No.
5. Account Type
6. Account Balance
7. F.D.No.

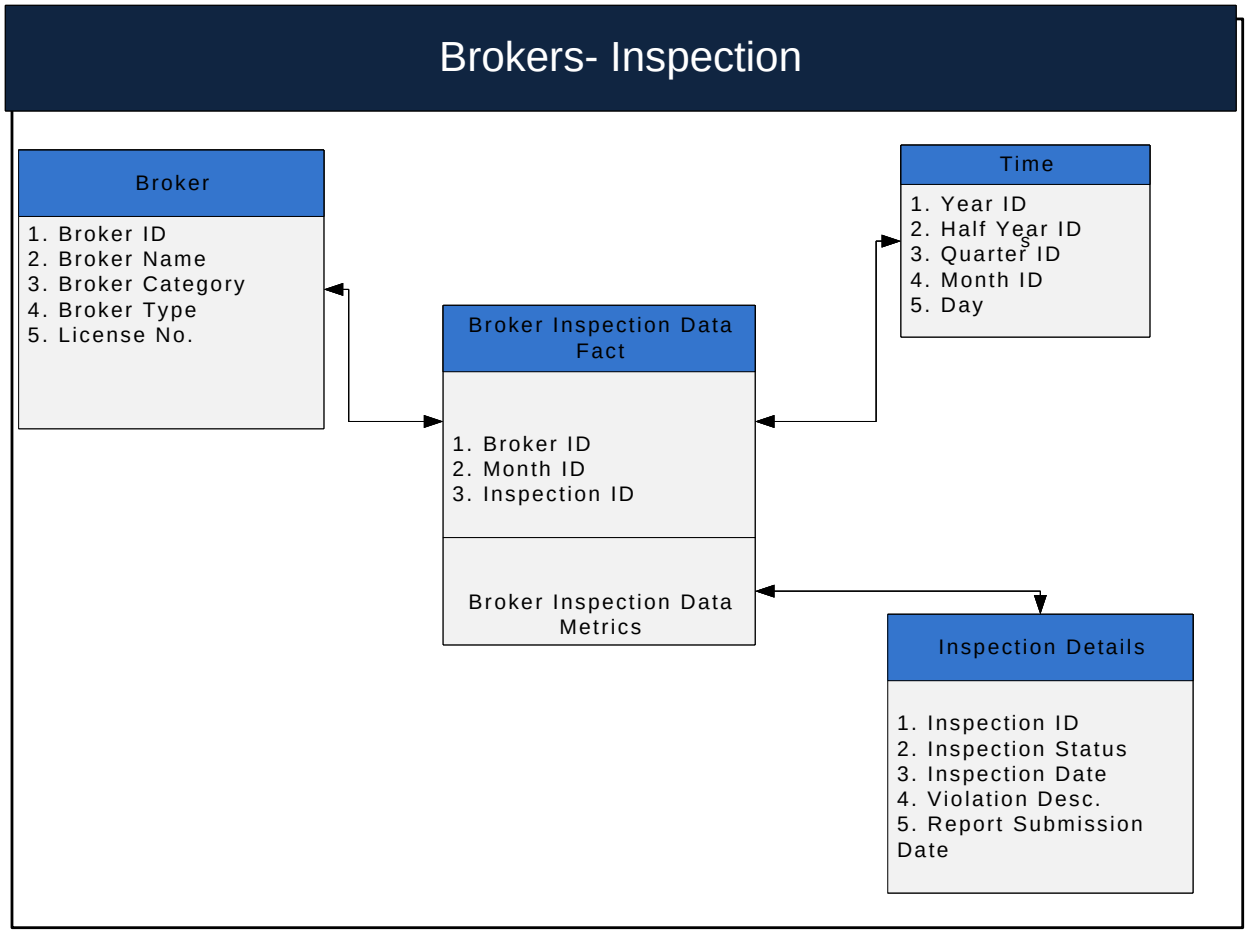
Associated Forms (Brokers Department)			
Code	**Form Name**	**Objective**	**Frequency**
INPUT_BROKER_1	Capital Structure and shareholders details for a broker	To capture the details of the capital structure of a broker	Quarterly
INPUT_BROKER_3	Financial Statement for each broker - Profit and Loss Statement	To capture the profit and loss statement details for a broker	Yearly
INPUT_BROKER_4	Balance Sheet of Brokers	To capture balance sheet details for a broker	Yearly
INPUT_BROKER_5	Financial data for brokers	To capture the financial data for a broker	Half Yearly
INPUT_BROKER_11	Insurance Bank Accounts of brokers	To capture the details of the insurance bank accounts	Yearly
INPUT_BROKER_15	Fixed Deposit Details	To capture the fixed deposit details for a broker	Yearly
INPUT_BROKER_19	Annual Fees Data	To capture the details of annual fees paid with details such as demand Draft details, date of payment and payment status.	Yearly

Dept.	Form Name	Dimensions			
		Broker	Time	Shareholder	Bank Details
Brokers	Capital Structure and shareholders details for a broker	X	Q	X	
	Financial Statement for each broker - Profit and Loss Statement	X	Y		
	Balance Sheet of Brokers	X	Y		
	Financial data for brokers	X	HY		
	Insurance Bank Accounts of brokers	X	Y		X
	Fixed Deposit Details	X	Y		X
	Annual Fees Data	X	Y		X


Brokers-Organization Structure Data
Broker
1. Broker ID
2. Broker Name
3. Broker Category
4. Broker Type
5. License No.
6. Name of Director/ Person(s)
7. Profession
8. Address
Broker Org Struct Fact
1. Broker ID
2. Year ID
Broker Org Struct Metrics
Time
1. Year ID
2. Half Year ID
3. Quarters ID
4. Month ID
5. Day

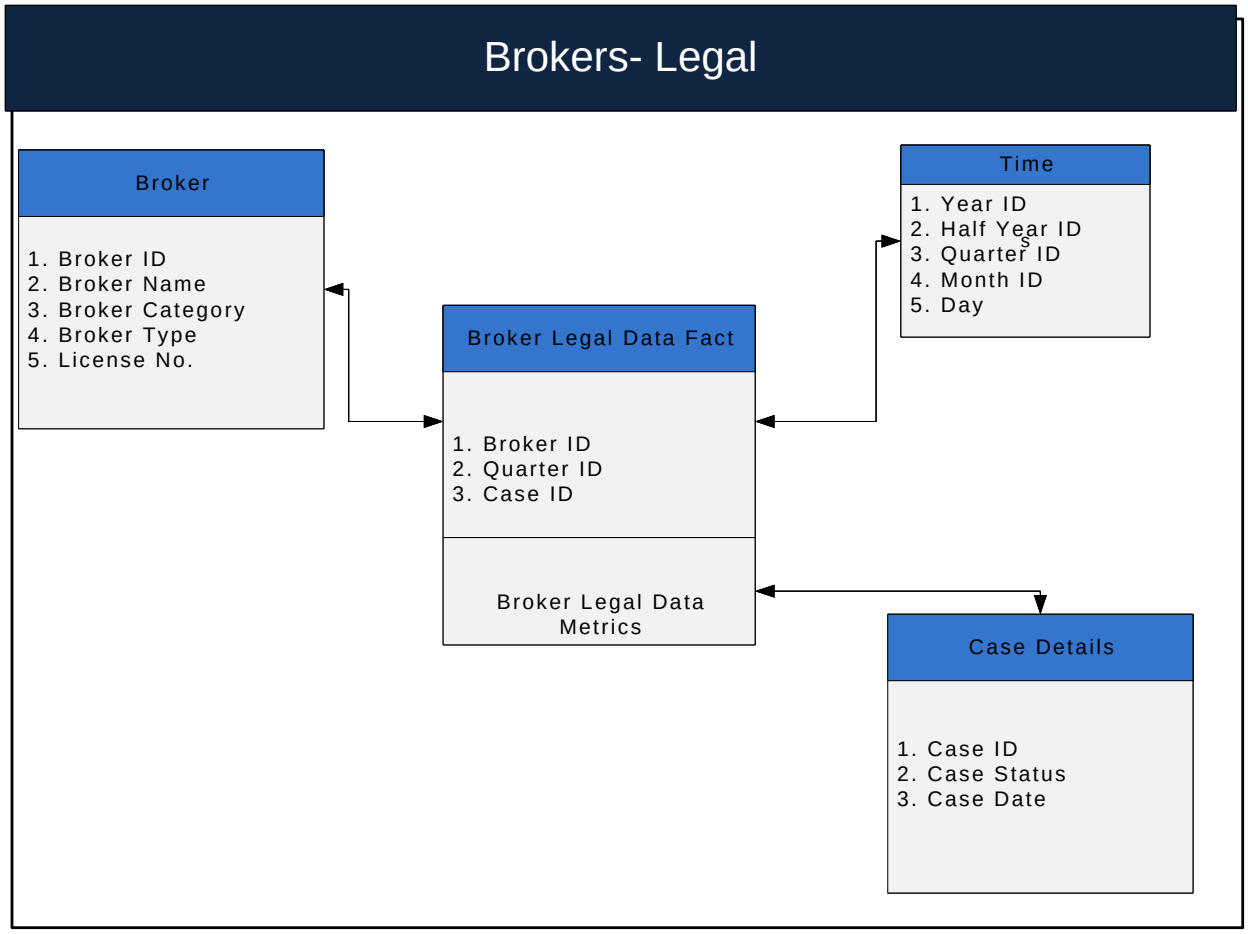
Associated Forms (Brokers Department)			
Code	**Form Name**	**Objective**	**Frequency**
INPUT_BROKER_6	Board of Directors and management details	To capture the details of the persons in the board of directors and management details	Yearly
INPUT_BROKER_8	Particulars of persons responsible for soliciting or procuring or broking insurance or reinsurance business	To capture the particulars of persons responsible for soliciting or procuring or broking insurance or reinsurance business	Yearly
INPUT_BROKER_9	Standing arrangements with other brokers or service providers	To capture the details of the standing arrangements with other brokers or service providers	Yearly
INPUT_BROKER_16	Details of Group companies for a broker	To capture the standing arrangements list of all group companies attached with a particular broker	Yearly

Dept.	Form Name	Dimensions	
		Broker	Time
Brokers	Board of Directors and management details	X	Y
	Particulars of persons responsible for soliciting or procuring or broking insurance or reinsurance business	X	Y
	Standing arrangements with other brokers or service providers	X	Y
	Details of Group companies for a broker	X	Y


Brokers- Inspection
Broker
1. Broker ID
2. Broker Name
3. Broker Category
4. Broker Type
5. License No.
Time
1. Year ID
2. Half Year ID
3. Quarter ID
4. Month ID
5. Day
Broker Inspection Data Fact
1. Broker ID
2. Month ID
3. Inspection ID
Broker Inspection Data Metrics
Inspection Details
1. Inspection ID
2. Inspection Status
3. Inspection Date
4. Violation Desc.
5. Report Submission Date

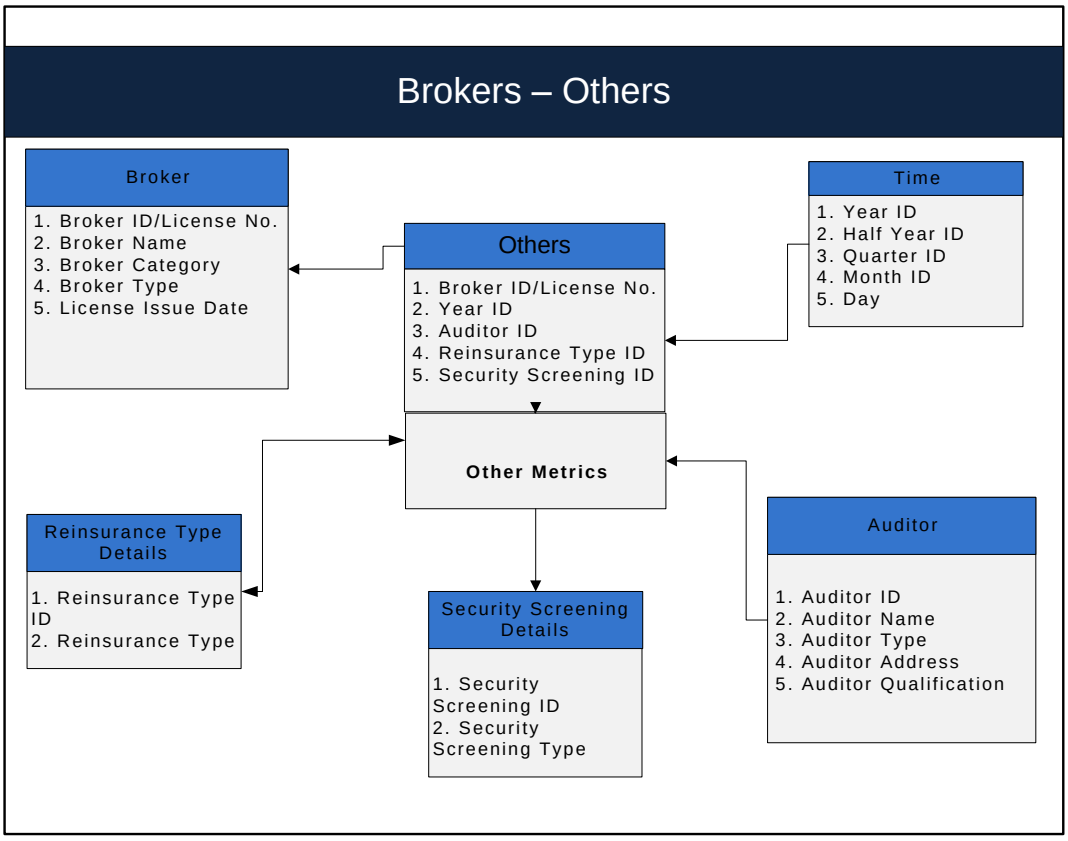
Associated Forms (Brokers Department)			
Code	**Form Name**	**Objective**	**Frequency**
INPUT_BROKER_17	Inspection Data	To capture the details of the inspection activities carried out against brokers	Monthly

Dept.	Form Name	Dimensions		
		Broker	Time	Inspection Details
Brokers	Inspection Data	X	M	X


Brokers- Legal
Broker
1. Broker ID
2. Broker Name
3. Broker Category
4. Broker Type
5. License No.
Time
1. Year ID
2. Half Year ID
3. Quarter ID
4. Month ID
5. Day
Broker Legal Data Fact
1. Broker ID
2. Quarter ID
3. Case ID
Broker Legal Data Metrics
Case Details
1. Case ID
2. Case Status
3. Case Date

Associated Forms (Brokers Department)			
Code	**Form Name**	**Objective**	**Frequency**
INPUT_BROKER_20	Legal Data	To capture the details of the no. of lawsuits against each broker	Quarterly

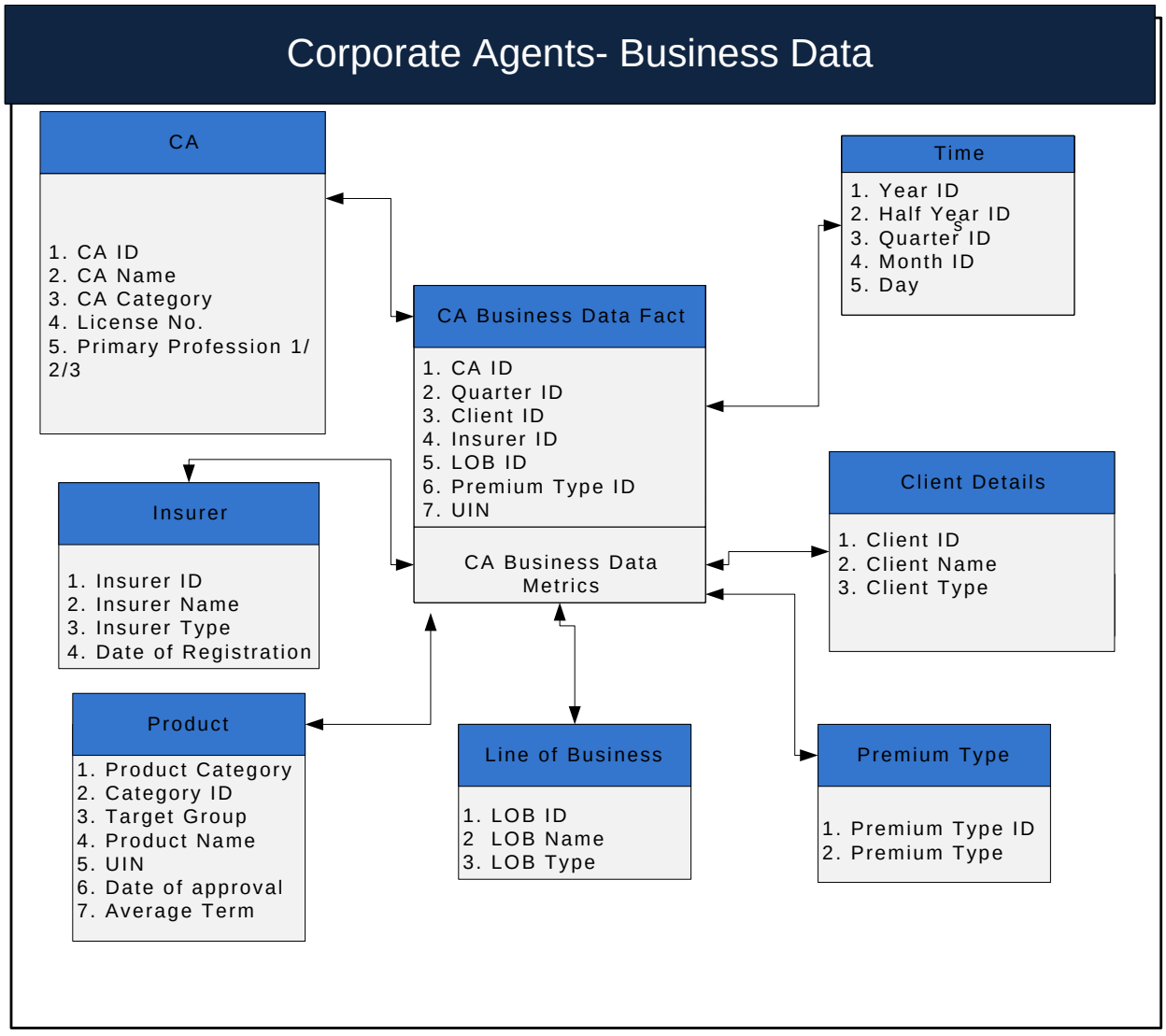
Dept.	Form Name	Dimensions		
		Broker	Time	Case Details
Brokers	Legal Data	X	Q	X


Brokers – Others
Broker
1. Broker ID/License No.
2. Broker Name
3. Broker Category
4. Broker Type
5. License Issue Date
Time
1. Year ID
2. Half Year ID
3. Quarter ID
4. Month ID
5. Day
Others
1. Broker ID/License No.
2. Year ID
3. Auditor ID
4. Reinsurance Type ID
5. Security Screening ID
Other Metrics
Reinsurance Type Details
1. Reinsurance Type ID
2. Reinsurance Type
Security Screening Details
1. Security Screening ID
2. Security Screening Type
Auditor
1. Auditor ID
2. Auditor Name
3. Auditor Type
4. Auditor Address
5. Auditor Qualification

Associated Forms (Brokers Department)			
Code	**Form Name**	**Objective**	**Frequency**
INPUT_BROKER_7	Audit arrangements for a broker	To capture the details of the audit arrangement for a broker.	Yearly
INPUT_BROKER_13	Reinsurance balances outstanding as at---	To capture the details of the reinsurance balances outstanding for a broker	Yearly
INPUT_BROKER_14	Security screening proceedings for reinsurance broking	To capture the details of the security screening proceedings for reinsurance banking	Yearly
INPUT_BROKER_21	APPLICATION FOR GRANT OF LICENCE/RENEWAL OF LICENCE	Each brokers who is willing to register with IRDA for broking business, is liable to fill up this form	As and when
INPUT_BROKER_22	GRANT OF LICENSE TO THE BROKERS	This form is used for granting license to a broker	As and when
INPUT_BROKER_23	APPLICATION FOR DUPLICATE LICENCE	This form is used for application for a duplicate license by the brokers	As and when

Dept.	Form Name	Dimensions				
		Broker	Time	Reinsurance Details	Auditor	Security Screening Details
Brokers	Audit arrangements for a broker	X	Y		X	
	Reinsurance balances outstanding as at---	X	Y	X		
	Security screening proceedings for reinsurance broking	X	Y			X
	APPLICATION FOR GRANT OF LICENCE/RENEWAL OF LICENCE	X	X			
	GRANT OF LICENSE TO THE BROKERS	X	X			
	APPLICATION FOR DUPLICATE LICENCE	X	X			

7. Intermediaries – Corporate Agents Department



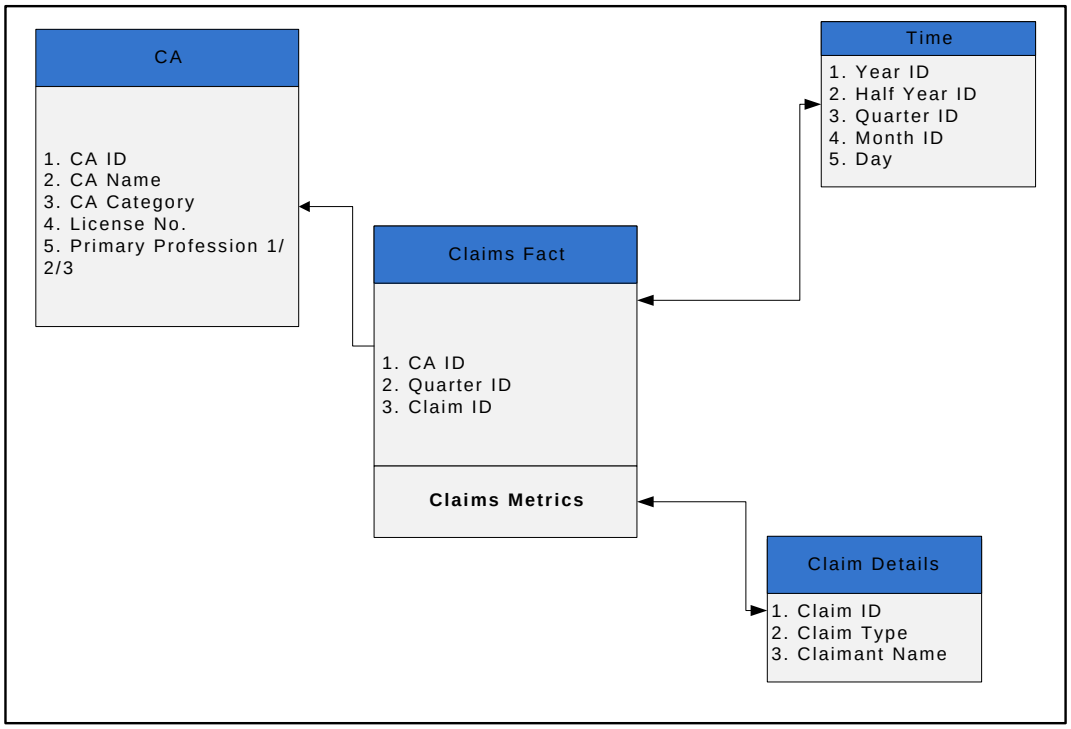
Associated Forms (CA Department)			
Code	**Form Name**	**Objective**	**Frequency**
INPUT_CA_14	New Business Data for corporate agents	To capture the new business data for a corporate agents insurer wise	Yearly
INPUT_CA_14.1	New Business Data for corporate agents(Insurer wise)	To capture the new business data for a corporate agent's insurer wise.	Quarterly

Dept.	Form Name	Dimensions						
		CA	Insurer	Time	Client	Premium Type	Product Category	LoB
CA	New Business Data for corporate agents	X	X	Y	X			
	New Business Data for corporate agents(Insurer wise)	X		Q		X	P	X

C: Category Level; P: Product level

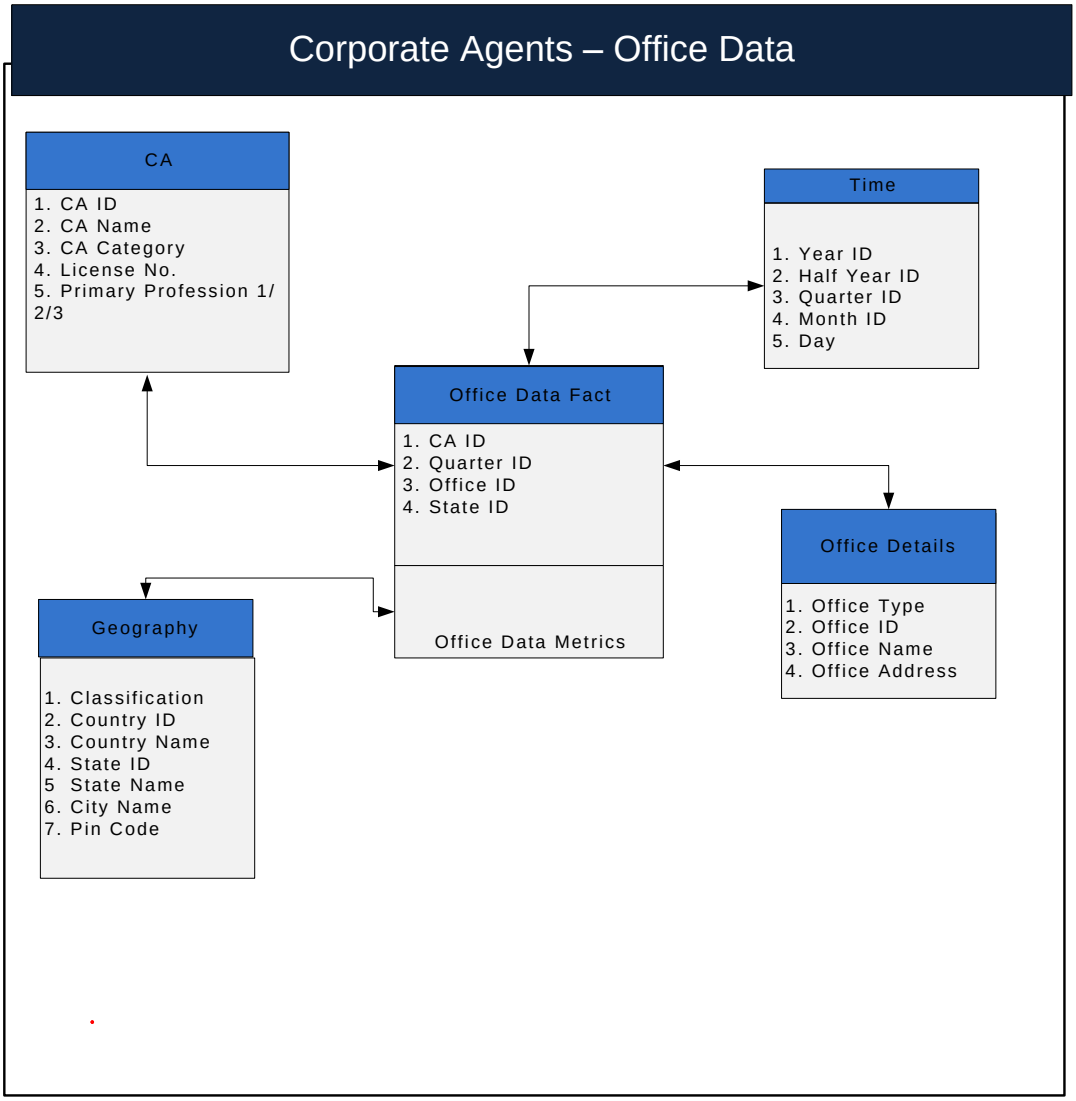
M: Monthly; Q: Quarterly; Y: Yearly

Corporate Agents– Claims Data



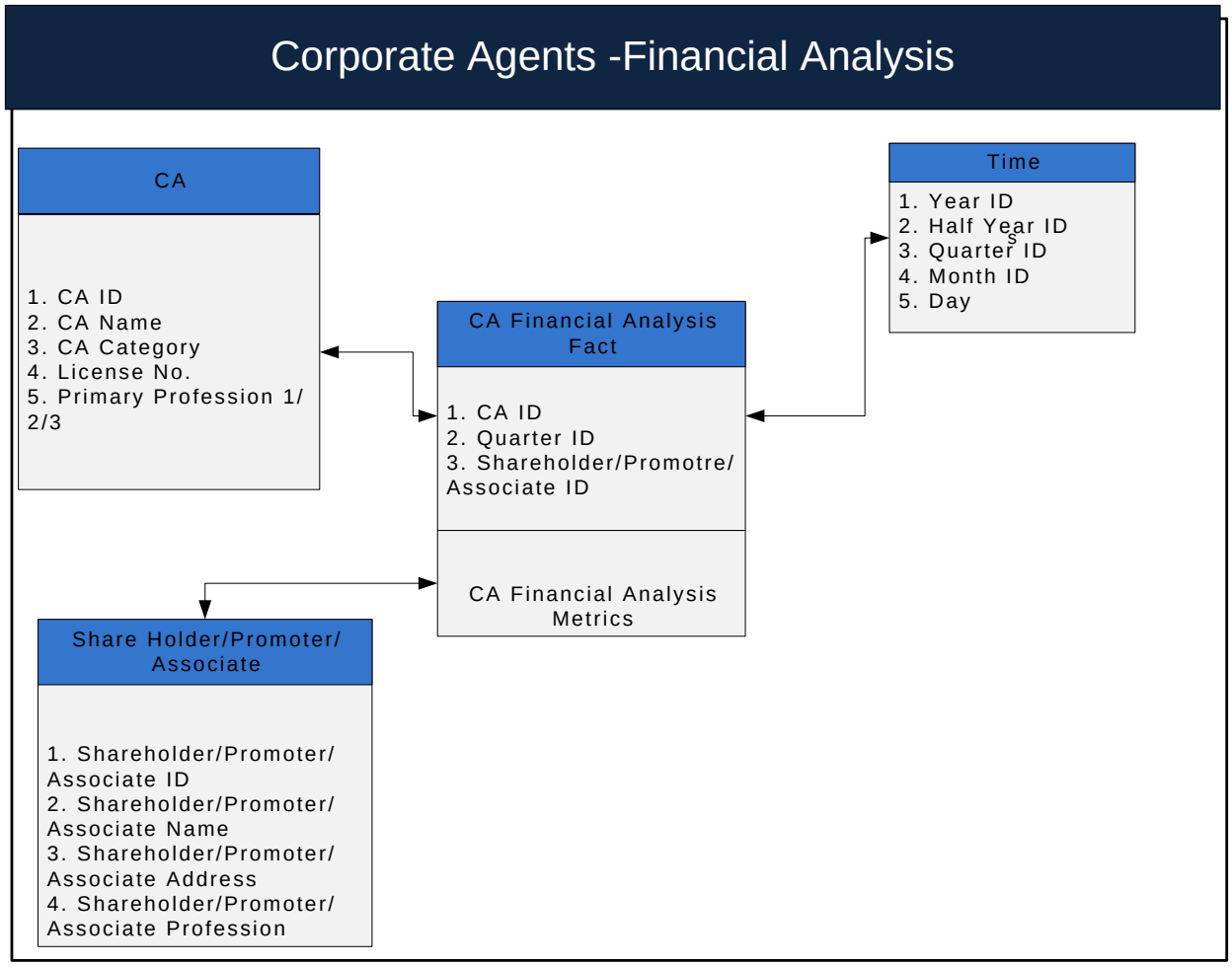
Associated Forms (CA Department)			
Code	**Form Name**	**Objective**	**Frequency**
INPUT_CA_13	Claims Data	To capture the details of the claims for a corporate agents	Quarterly

Dept.	Form Name	Dimensions		
		CA	Claim Details	Time
CA	Claims Data	X	X	Q


Corporate Agents – Office Data
CA
1. CA ID
2. CA Name
3. CA Category
4. License No.
5. Primary Profession 1/ 2/3
Time
1. Year ID
2. Half Year ID
3. Quarter ID
4. Month ID
5. Day
Office Data Fact
1. CA ID
2. Quarter ID
3. Office ID
4. State ID
Office Data Metrics
Office Details
1. Office Type
2. Office ID
3. Office Name
4. Office Address
Geography
1. Classification
2. Country ID
3. Country Name
4. State ID
5 State Name
6. City Name
7. Pin Code

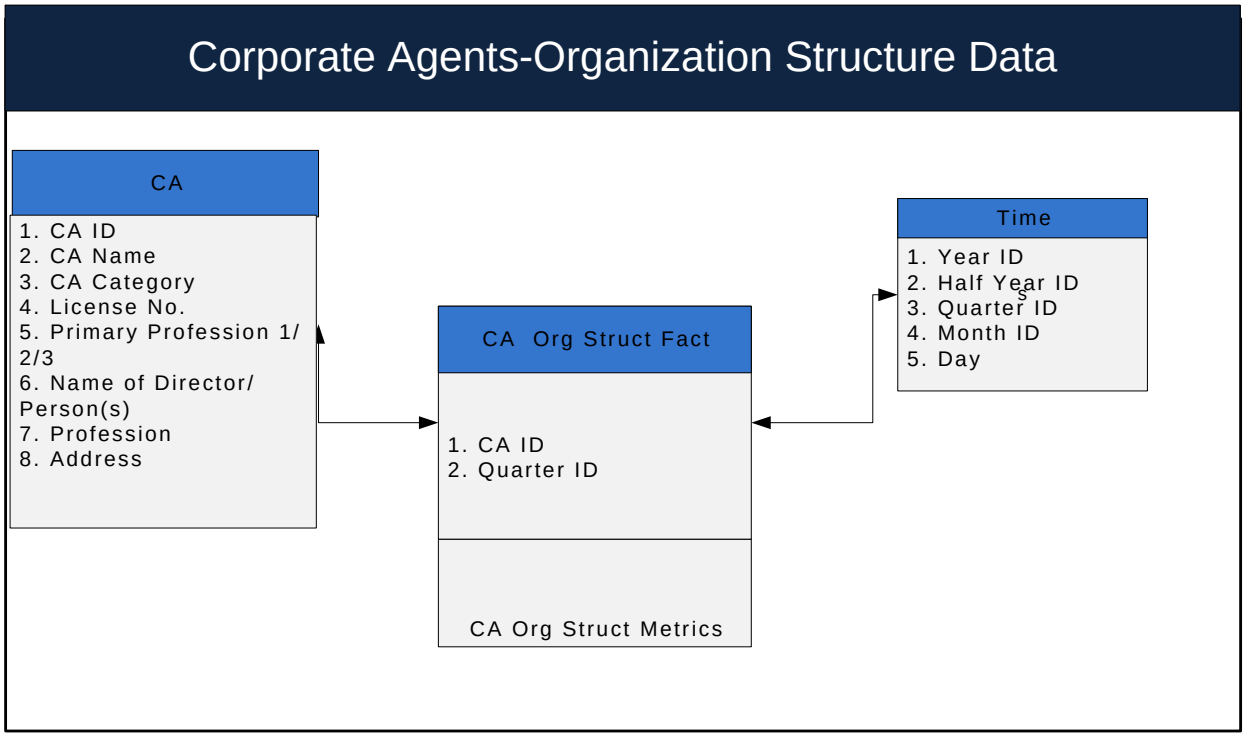
Associated Forms (CA Department)			
Code	**Form Name**	**Objective**	**Frequency**
Input_CA_12.0	Particular of offices of corporate agents	To capture the details of an office for a corporate agent	Yearly

Dept.	Form Name	Dimensions			
		CA	Geography	Office	Time
CA	Particular of offices of corporate agents	X	X	X	Y


Corporate Agents -Financial Analysis
CA
1. CA ID
2. CA Name
3. CA Category
4. License No.
5. Primary Profession 1/ 2/3
Time
1. Year ID
2. Half Year ID
3. Quarter ID
4. Month ID
5. Day
CA Financial Analysis Fact
1. CA ID
2. Quarter ID
3. Shareholder/Promotre/ Associate ID
CA Financial Analysis Metrics
Share Holder/Promoter/ Associate
1. Shareholder/Promoter/ Associate ID
2. Shareholder/Promoter/ Associate Name
3. Shareholder/Promoter/ Associate Address
4. Shareholder/Promoter/ Associate Profession

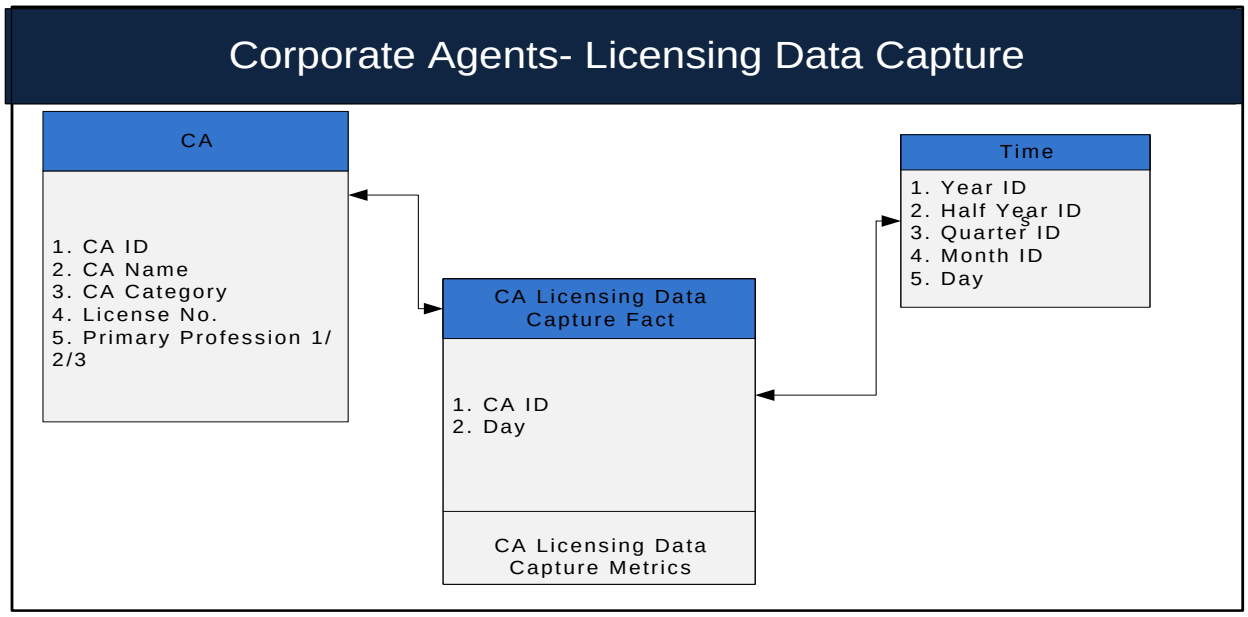
Associated Forms (CA Department)			
Code	**Form Name**	**Objective**	**Frequency**
Input_CA_10.0	Income Statement	To capture financial data for inflow and outflow with respect to a corporate agent	Yearly
Input_CA_10.1	Balance Sheet	To capture balance sheet data for a corporate agent	Yearly
Input_CA_11.0	Capital structure and Shareholder's Details of a corporate agents	To capture the details of the capital structure and shareholders for a corporate agent	Quarterly
Input_CA_11.1	Income Data	To capture the income data for the corporate agents	Yearly

Dept.	Form Name	Dimensions		
		CA	Time	Shareholder /Promoter
CA	to capture the income data for the corporate agents	X	Y	
	to capture the income data for the corporate agents	X	Y	
	to capture the income data for the corporate agents	X	Q	X
	to capture the income data for the corporate agents	X	Y	


Corporate Agents-Organization Structure Data
CA
1. CA ID
2. CA Name
3. CA Category
4. License No.
5. Primary Profession 1/ 2/3
6. Name of Director/ Person(s)
7. Profession
8. Address
CA Org Struct Fact
1. CA ID
2. Quarter ID
CA Org Struct Metrics
Time
1. Year ID
2. Half Year ID
3. Quarter ID
4. Month ID
5. Day

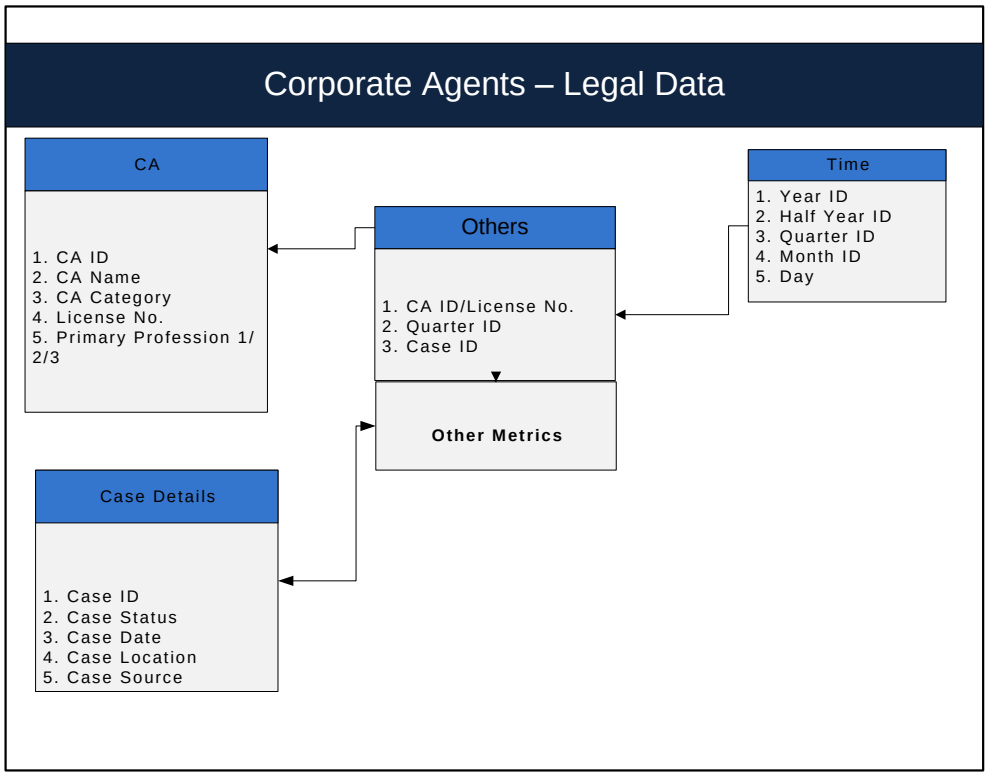
Associated Forms (CA Department)			
Code	**Form Name**	**Objective**	**Frequency**
Input_CA_7.0	Board of Director and management details	To capture the details of the board of directors / partners for a corporate agent and management details	Yearly
Input_CA_8.0	Particulars of specified persons responsible for soliciting or procuring or insurance or reinsurance business	To the particulars of specified persons responsible for soliciting or procuring or insurance or reinsurance business	Yearly
Input_CA_9.0	Group Companies for a corporate agent	To capture list of all group companies attached with a corporate agent	Yearly

Dept.	Form Name	Dimensions	
		CA	Time
CA	Board of Director and management details	X	Y
	Particulars of specified persons responsible for soliciting or procuring or insurance or reinsurance business	X	Y
	Group Companies for a corporate agent	X	Y


Corporate Agents- Licensing Data Capture
CA
1. CA ID
2. CA Name
3. CA Category
4. License No.
5. Primary Profession 1/ 2/3
Time
1. Year ID
2. Half Year ID
3. Quarter ID
4. Month ID
5. Day
CA Licensing Data Capture Fact
1. CA ID
2. Day
CA Licensing Data Capture Metrics

Associated Forms (CA Department)			
Code	**Form Name**	**Objective**	**Frequency**
INPUT_CA_1	Application for a new license to act as a Corporate Agent	This form is used for application for a new corporate agent license.	As and when required
INPUT_CA_2	Application for a License/ Renewal of License to act as a Corporate Agent	This form is used for application for a license/renewal of license to act as a corporate agent	As and when required
INPUT_CA_3	License to Act as a specified person under the Insurance Act, 1938 (IV OF 1938)	This form is used for application from a firm or company for a certificate/renewal of certificate to act as a specified person	As and when required
INPUT_CA_4	License to Act as a Corporate Agent under the Insurance Act, 1938 (IV OF 1938)	This form is used for issuing license to act as a corporate agent	As and when required
INPUT_CA_5	Data Capture for Corporate Agents	To capture the details like name, address, contact no., photograph, date of commencement of employment, date of leaving the service, if any, and salary specified for a corporate agent.	As and when required
INPUT_CA_6	Application for Duplicate License	The form will be used for application of a duplicate license in case the original license gets destroyed or lost or mutilated	As and when required

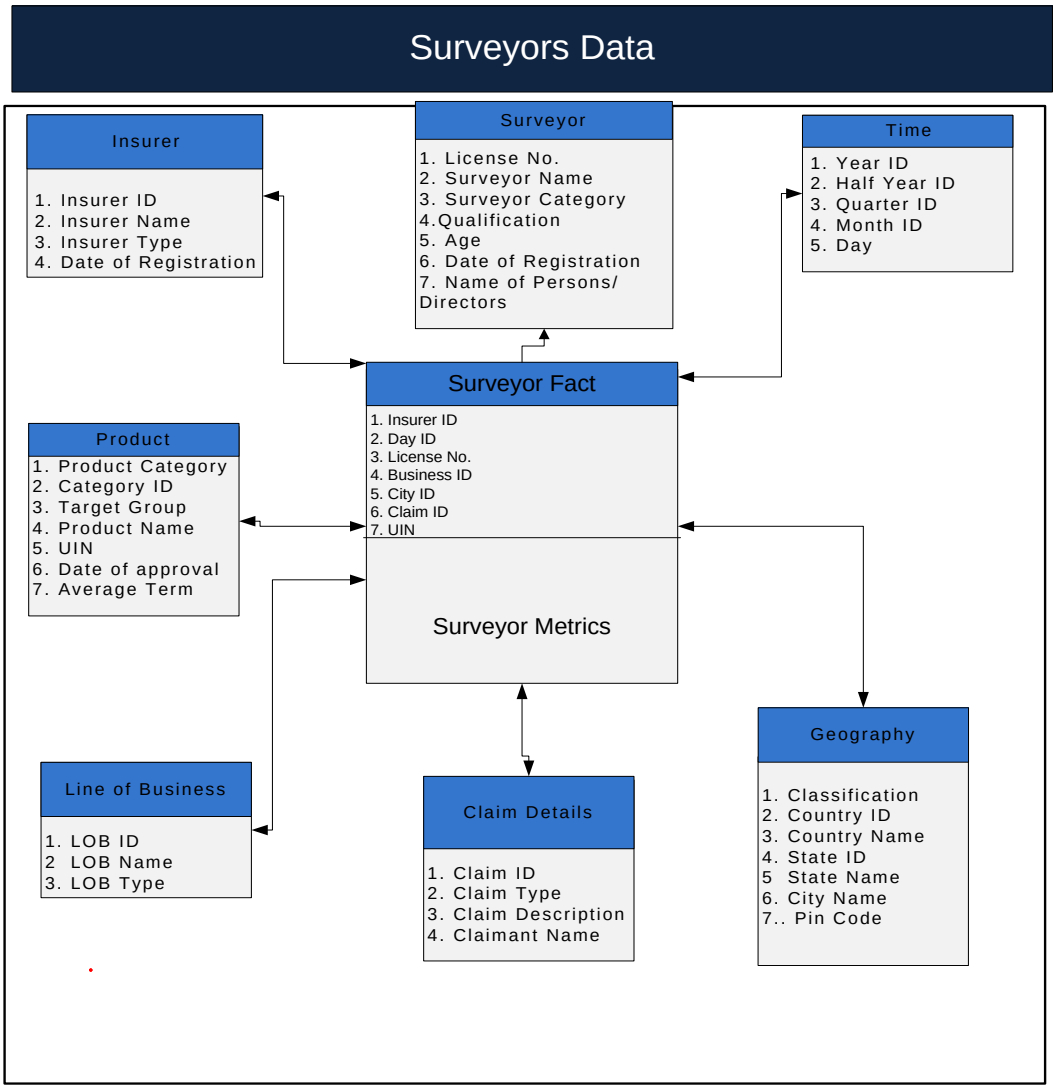
Dept.	Form Name	Dimensions	
		CA	Time
CA	Application for a new license to act as a Corporate Agent	X	D
	Application for a License/ Renewal of License to act as a Corporate Agent	X	D
	License to Act as a specified person under the Insurance Act, 1938 (IV OF 1938)	X	D
	License to Act as a Corporate Agent under the Insurance Act, 1938 (IV OF 1938)	X	D
	Data Capture for Corporate Agents	X	D
	Application for Duplicate License	X	D


Corporate Agents – Legal Data
CA
1. CA ID
2. CA Name
3. CA Category
4. License No.
5. Primary Profession 1/ 2/3
Others
1. CA ID/License No.
2. Quarter ID
3. Case ID
Other Metrics
Time
1. Year ID
2. Half Year ID
3. Quarter ID
4. Month ID
5. Day
Case Details
1. Case ID
2. Case Status
3. Case Date
4. Case Location
5. Case Source

Associated Forms (CA Department)			
Code	**Form Name**	**Objective**	**Frequency**
Input_CA_16.0	Legal Data for Corporate Agents	To capture the details of the no. of lawsuits against each corporate agent	Quarterly

Dept.	Form Name	Dimensions		
		Broker	Time	Claim Details
CA	Legal Data for Corporate Agents	X	Q	X

8. Intermediaries – Surveyors



Associated Forms (Surveyor Department)			
Code	**Form Name**	**Objective**	**Frequency**
Form 1-AF	APPLICATION FOR A LICENCE TO ACT AS SURVEYOR AND LOSS ASSESSOR	To capture details of an applicant in the application process	As and When
FORM - IRDA – 3A – AF	Details of partners / directors for a surveying firm	To capture the details of partners / directors for a surveying firm	Yearly
Form - IRDA- 2-AF	APPLICATION FROM A FIRM OR COMPANY FOR A LICENCE TO ACT AS A SURVEYOR AND LOSS ASSESSOR	To capture details of an applicant in the application process from a firm or a company	As and When
Form - IRDA- 5-AF	APPLICATION FOR RENEWAL OF A LICENCE TO ACT AS SURVEYOR AND LOSS ASSESSOR	To capture the details of the surveyor for renewal of license	As and When
Form - 6A-AF	APPLICATION FROM A FIRM OR COMPANY FOR RENEWAL OF A LICENCE TO ACT AS A SURVEYOR AND LOSS ASSESSOR	To capture the details of the surveyor for renewal of license(In case of firm or a company)	As and When
Form 3-AF	APPLICATION FROM A FIRM OR COMPANY FOR A	To capture the details of fresh application for a firm or a company	As and When

Associated Forms (Surveyor Department)			
Code	**Form Name**	**Objective**	**Frequency**
	LICENCE TO ACT AS A SURVEYOR AND LOSS ASSESSOR		
FORM - IRDA – 9	Application for Duplicate License	To capture application details for duplicate license	As and When
FORM - IRDA – 13	Data capture format for capturing 3 years of data	To capture state wise information for each surveyor for claims and inspections data	Yearly
Form III	PRESCRIBED FORMAT FOR ENROLLMENT OF TRAINEE SURVEYORS & LOSS ASSESSORS FOR TRAINING	To capture the enrollment details for a trainee surveyor	As and When
Form IV	FORMAT FOR DAILY DIARY	To capture the quarterly data for a trainee surveyor having details of the training activities	Quarterly

		Insurer	Product	LoB	Surveyor	Claim	Geography	Time
Surveyor	APPLICATION FOR A LICENCE TO ACT AS SURVEYOR AND LOSS ASSESSOR			X	X		X	D
	Details of partners / directors for a surveying firm			X	X		X	Y
	APPLICATION FROM A FIRM OR COMPANY FOR A LICENCE TO ACT AS A SURVEYOR AND LOSS ASSESSOR			X	X		X	D
	APPLICATION FOR RENEWAL OF A LICENCE TO ACT AS SURVEYOR AND LOSS ASSESSOR			X			X	D
	APPLICATION FROM A FIRM OR COMPANY FOR RENEWAL OF A LICENCE TO ACT AS A SURVEYOR AND LOSS ASSESSOR			X				D
	APPLICATION FROM A FIRM OR COMPANY FOR A LICENCE TO ACT AS A SURVEYOR AND LOSS ASSESSOR			X	X		X	D
	Application for Duplicate License			X				D
	Data capture format for capturing 3 years of data	X	P	X	X	X	X	Y
	PRESCRIBED FORMAT FOR ENROLLMENT OF TRAINEE SURVEYORS & LOSS ASSESSORS FOR TRAINING			X	X		X	D
	FORMAT FOR DAILY DIARY			X	X		X	Q

B. Indicative List of Dimensions with their values and attributes

Dimensions Used	Important Attributes	Attribute Definition
Time	Year ID	Calendar or Financial Year
	Half Year	Half Year within a Year
	Quarter ID	Quarter of a year
	Month ID	Month of a year
	Day	Days and Dates within a year
Insurer	Insurer ID	Unique Identification Number of an Insurer
	Insurer Name	Name of an Insurer
	Insurer Type	Category or Type in which the Insurer belongs. For example, private insurer, public sector insurer
	Date of Registration	Date of Registration for an Insurer
Reinsurer	Reinsurer ID	Unique Identification Number of a Reinsurer
	Reinsurer Name	Name of a Reinsurer
	Reinsurer Type	Category or Type in which the Reinsurer belongs. For example, private insurer, public sector insurer
	Date of Registration	Date of Registration for a Reinsurer
Geography	Country ID	Unique identifier for a country
	Country Name	Name of the country
	Classification	Within India or Outside India Business
	State ID	Unique Identification Number of department for a state within the country
	State Name	Name of the State

Dimensions Used	Important Attributes	Attribute Definition
	City Name	Name of the city
	Pin Code	Unique code for a city
Product	Product Category ID	Unique ID for the product category
	Product Category Name	Name of the product category
	Target Group of the Product	Target group which the products belongs to
	Product UIN	Unique identification number assigned with each product approved by IRDA
	Product Name	Name of the product
	Date of Approval	Date of approval of the product by IRDA
	Average Term	Average of the term of the product
Line of Business	Business ID	Unique Identification Number of department or a line of business
	Business Name	Name of the line of Business
	Business Type	Category or Type in which the business belongs. For example, rural or urban etc.
Premium Type	Premium Type ID	Unique ID for each of the premium type
	Premium Type	Type of the premium
Division	Division ID	Unique Identifier for a division
	Division Name	Label of a particular division
Channel Type	Channel ID	Unique ID for identifying each of the different channel type
	Channel Name	The name of the channel used for acquiring business
Claim Details	Claim ID	Unique Identifier for a claim

Dimensions Used	Important Attributes	Attribute Definition
	Claim Type	Name of the claim
	Claimant Name	The name of the claimant
	Claim Description	Description of the claim
Location Type	Location ID	Unique identifier for a location type
	Location Name	Name of a location type
Group	Group ID	Unique Identifier for a group
	Group Name	Name of the group
Office Details	Office ID	Unique ID for identifying each of the different channel type
	Office Type	The name of the channel used for acquiring business
	Office Name	Unique ID generated for each policy slab
	Office Address	Complete postal address of the office
Location	Location ID	Unique identifier for the location
	Location Name	Name and type of the location
Policy Slab	Slab ID	Unique ID generated for each policy slab
	Slab Name	Detailed description for each policy slab
Advertisement Details	URN	
	Date of Launch	Date of launch of the advertisement
	Ad Type	
	Co Insurer	
	Medium	
Case Details	Case ID	Unique Identification Number of a case
	Case Source	Source of the case

Dimensions Used	Important Attributes	Attribute Definition
	Case Location	Location where the case took place
	Case Status	Current Status of the case
	Case Date	Date of registration of the case
CA	CA ID	Unique Identification Number of a corporate agent
	CA Name	Name of a corporate agent
	CA Category	Category in which the corporate agent belongs.
	License No.	License number of the corporate agent
	Primary Profession 1/2/3	Primary Profession of the corporate agent
Auditor	Auditor ID	Unique Identification Number of an auditor
	Auditor Name	Name of a auditor
	Auditor Type	Type of auditor
	Auditor Address	Address of auditor
	Auditor Qualification	Profession of auditor
Reinsurance Details	Reinsurance Details ID	Unique Identification Number of Reinsurance Details
	Reinsurance Details Name	Name of the Reinsurance Details
Security Screening	Security Screening ID	Unique Identification Number of a Security Screening
	Security Screening Name	Name of a Security Screening type
	Average Term	Average of the term of the product
Broker	Broker ID	Unique Identification Number of an Broker

Dimensions Used	Important Attributes	Attribute Definition
	Broker Name	Name of an Broker
	Broker Category	Category in which the Broker belongs. For example, private broker, public sector broker
	License No.	License number of the broker
	Broker Type	Type in which the Broker belongs
Client Details	Client ID	Unique ID for each of the client
	Client Type	Type of the client
	Client name	Name of the client
TPA	TPA ID	Unique Identification Number of a TPA
	TPA Name	Name of a TPA
	Date of Registration	Date of Registration for a TPA
Cover Type	Cover Type ID	Unique ID for identifying each of the different cover type
	Cover Type Name	The name of the cover type used for acquiring business
Shareholder	Shareholder ID	Unique Identification Number of Shareholder
	Shareholder Name	Name of the Shareholder
	Shareholder Address	Postal Address of the Shareholder
	Shareholder Category	Category of the Shareholder
	Shareholder Profession	Profession of the Shareholder
Bank Details	Bank ID	Unique Identification Number of bank
	Bank Name	Name of the bank

Dimensions Used	Important Attributes	Attribute Definition
	Bank Address	Postal Address of the bank
	Account No.	Unique Identification Number of account
	Account Type	Category of the account
	Account Balance	Current account balance
	F.D. No.	Unique Identification Number of F.D.
Shareholder/Promoter /Associate	Shareholder ID	Unique Identification Number of Shareholder/Promoter/Associate
	Shareholder Name	Name of the Shareholder/Promoter/Associate
	Shareholder Address	Postal Address of the Shareholder/Promoter/Associate
	Shareholder Profession	Profession of the Shareholder/Promoter/Associate
Inspection Details	Inspection ID	Unique Identification Number of inspection being carried out
	Inspection Status	Current status of the inspection activity
	Inspection Date	Date of carrying out the inspection activity
	Violation Desc	Detailed description of the violation occurred
	Report Submission Date	Date of submission of the report
Treaty Details	Treaty ID	Unique Identification Number of the treaty
	Treaty Type	Type of the treaty
	Treaty Name	Name of the treaty
	Nature of Treaty	Nature of the treaty
	Basis of Treaty	Basis of the treaty

Dimensions Used	Important Attributes	Attribute Definition
SubClass Details	SubClass ID	Unique Identification Number of the subclass
	SubClass Name	Name of the subclass
Surveyor	License Number	Unique Identification Number of a Surveyor
	Surveyor Name	Name of a Surveyor
	Surveyor category	Category or Type in which the Surveyor belongs.
	Date of Registration	Date of Registration for a Surveyor
	Age	Age of a Surveyor
	Qualification	Qualification of a Surveyor
	Name of Persons/Directors	
Actuary	Actuary ID	Unique Identification Number of an Actuary
	Actuary Name	Name of a Actuary
Rating Agency	Rating Agency ID	Unique Identification Number of a rating agency
	Rating Agency Name	Name of a rating agency

C. Data Sizing Estimate for the IRDA BAP Solution

Generic Assumptions:

- Average Row Size = 0.5 KB (Assuming a maximum of 15 columns in a table)
- Data type for each field: VarChar(25)
- No. of years of history data: 8
- Growth of data per year till date = 8%
- No. of years of future data: 5
- No. of Product Categories: 2
- No. of divisions: 2
- No. of groups: 2
- No. of states: 30
- No. of premium types: 4
- No. of channels: 8

a) Life Department

Key Assumptions

- No. of Insurers=30
- No. of Products per Insurer=50
- No of Repudiated Claims per Insurer per Quarter=20
- No. of lines of business: 4

Subject Area	Master Data Combinations (Possible)	Approximate No. of Data Point Inputs	Total Row Size(GB)	% Monthly data	Monthly Data (GB)	% of Quarterly data	Quarterly Data (GB)	% of Yearly data	Yearly Data (GB)	Total Data(GB)
NB	2880000.00	8.00	10.99	0.00	0.00	0.78	34.28	0.22	2.42	36.69
RNB	48000.00	8.00	0.18	0.00	0.00	1.00	0.73	0.00	0.00	0.73
Claims Data	1152000.00	20.00	10.99	0.00	0.00	1.00	43.95	0.00	0.00	43.95
Agency Stats	36000.00	10.00	0.17	0.00	0.00	1.00	0.69	0.00	0.00	0.69
Office Data	300000.00	10.00	1.43	1.00	17.17	0.00	0.00	0.00	0.00	17.17
Advertisement Data	7200.00	4.00	0.01	1.00	0.16	0.00	0.00	0.00	0.00	0.16
Others	3840.00	20.00	0.04	0.00	0.00	1.00	0.15	0.00	0.00	0.15

Department Total = 99.54 GB

b) Non Life General Department

Key Assumptions

- No. of Insurers=30
- No. of Products per Insurer=50
- No of Repudiated Claims per Insurer per Quarter=20
- No. of lines of business = 10

Subject Area	Master Data Combinations (Possible)	Approximate No. of Data Point Inputs	Total Row Size(GB)	% Monthly data	Monthly Data (GB)	% of Quarterly data	Quarterly Data (GB)	% of Yearly data	Yearly Data (GB)	Total Data(GB)
NB Data	288000.00	8.00	1.10	0.00	0.00	1.00	4.39	0.00	0.00	4.39
Product Performance Data	60000.00	40.00	1.14	0.00	0.00	0.00	0.00	1.00	1.14	1.14
Claims Data	48000.00	20.00	0.46	0.00	0.00	1.00	1.83	0.00	0.00	1.83
Non Life MI	6000.00	10.00	0.03	0.00	0.00	1.00	0.11	0.00	0.00	0.11
Office Data	36000.00	10.00	0.17	0.00	0.00	1.00	0.69	0.00	0.00	0.69

Department Total = 8.17 GB

c) Non Life Reinsurance Department

Key Assumptions

- No. of Insurers=30
- No. of Reinsurers=15
- No. of Treaties per Quarter=50
- No. of Products per Quarter=50
- No. of lines of business = 10

Subject Area	Master Data Combinations (Possible)	Approximate No. of Data Point Inputs	Total Row Size(GB)	% Monthly data	Monthly Data (GB)	% of Quarterly data	Quarterly Data (GB)	% of Yearly data	Yearly Data (GB)	Total Data(GB)
Treaty Wise Data	11250000.00	10.00	53.64	0.00	0.00	0.00	0.00	1.00	53.64	53.64
Program Details	2250000.00	5.00	5.36	0.00	0.00	0.00	0.00	1.00	5.36	5.36
Business Data	15000.00	6.00	0.04	0.00	0.00	0.00	0.00	1.00	0.04	0.04
Recoveries Data	225000.00	10.00	1.07	0.00	0.00	0.50	2.15	0.50	0.54	2.68
Claims Data	9000.00	10.00	0.04	0.00	0.00	1.00	0.17	0.00	0.00	0.17
Others	4500.00	10.00	0.02	0.00	0.00	1.00	0.09	0.00	0.00	0.09

Department Total = 61.99 GB

d) Health Department

Key Assumptions

- No. of TPAs=30
- No. of Insurers=30
- No. of Products per Quarter=50
- No. of lines of business = 10

Subject Area	Master Data Combinations (Possible)	Approximate No. of Data Point Inputs	Total Row Size(GB)	% Monthly data	Monthly Data (GB)	% of Quarterly data	Quarterly Data (GB)	% of Yearly data	Yearly Data (GB)	Total Data(GB)
Business Data	72000.00	6.00	0.21	0.00	0.00	1.00	0.82	0.00	0.00	0.82
Product Performance Data	1152000.00	10.00	5.49	0.00	0.00	0.00	0.00	1.00	5.49	5.49
Claims Data	9000.00	10.00	0.04	0.60	0.31	0.00	0.00	0.40	0.02	0.33
TPA Data	4500.00	10.00	0.02	0.33	0.08	0.00	0.00	0.67	0.01	0.10
TPA Financial Data	27000.00	50.00	0.64	0.00	0.00	0.25	0.64	0.75	0.48	1.13

Department Total = 7.87 GB

e) Actuarial Department

Key Assumptions

- No. of Insurers=30
- No. of reinsurers=15
- No. of Products per Insurer=50
- No. of lines of business = 10

Subject Area	Master Data Combinations (Possible)	Approximate No. of Data Point Inputs	Total Row Size(GB)	% Monthly data	Monthly Data (GB)	% of Quarterly data	Quarterly Data (GB)	% of Yearly data	Yearly Data (GB)	Total Data(GB)
IBNR	6000.00	10.00	0.03	0.00	0.00	1.00	0.11	0.00	0.00	0.11
Valuations	1800000.00	10.00	8.58	0.00	0.00	0.00	0.00	1.00	8.58	8.58
Reinsurance	2250000.00	10.00	10.73	0.00	0.00	0.00	0.00	1.00	10.73	10.73

Department Total = 19.43 GB

f) Intermediaries- Brokers Department

Key Assumptions

- No. of Brokers=300
- No. of broker categories = 4
- No. of Insurers=30

Subject Area	Master Data Combinations (Possible)	Approximate No. of Data Point Inputs	Total Row Size(GB)	% Monthly data	Monthly Data (GB)	% of Quarterly data	Quarterly Data (GB)	% of Yearly data	Yearly Data (GB)	Total Data(GB)
Business Data	4320000.00	8.00	16.48	0.00	0.00	0.33	21.75	0.67	11.04	32.79
Claims Data	300000.00	4.00	0.57	0.00	0.00	1.00	2.29	0.00	0.00	2.29
Office Data	150000.00	4.00	0.29	0.00	0.00	0.00	0.00	1.00	0.29	0.29
Financial data	300000.00	10.00	1.43	0.00	0.00	0.00	0.00	1.00	1.43	1.43
Organization Structure Data	300.00	10.00	0.00	0.00	0.00	0.00	0.00	1.00	0.00	0.00
Inspection Data	300.00	10.00	0.00	1.00	0.02	0.00	0.00	0.00	0.00	0.02
Legal Data	15000.00	10.00	0.07	0.00	0.00	1.00	0.29	0.00	0.00	0.29
Others	15000.00	10.00	0.07	0.00	0.00	0.00	0.00	1.00	0.07	0.07

Department Total = 37.18 GB

g) F&A Department

Key Assumptions

- No. of Insurers=30
- No. of shareholders for an insurer = 50

Subject Area	Master Data Combinations (Possible)	Approximate No. of Data Point Inputs	Total Row Size(GB)	% Monthly data	Monthly Data (GB)	% of Quarterly data	Quarterly Data (GB)	% of Yearly data	Yearly Data (GB)	Total Data(GB)
Financial Data	6000.00	15.00	0.04	0.00	0.00	0.00	0.00	1.00	0.04	0.04
Shareholder's Data	15000.00	10.00	0.07	0.00	0.00	1.00	0.29	0.00	0.00	0.29
NB Data (Life)	3840.00	6.00	0.01	1.00	0.13	0.00	0.00	0.00	0.00	0.13
NB Data (Non Life)	1200.00	6.00	0.00	1.00	0.04	0.00	0.00	0.00	0.00	0.04

Department Total = 0.5 GB

Approximate data size for the current year (including all the departments and functions) = 317 GB

Total data size (Considering 8 years of history data at 8% growth) = 317*8/ (1.08^7) = 1.48 TB

Indexing Factor = 8%

Total Adjusted Data Size Considering Indexing= 1.48*(1.08) = 1.58 TB

h) Total physical space Estimation

Assuming a physical space of 70% of the total data size is consumed by the logs, views, stored procedures and tables etc., the YoY estimation of the total space is given below:

	Year wise data size (in TB)							
	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Year 8
Aggressive Estimate (12% Growth in Data Per Year)	2.7	3.0	3.4	3.8	4.2	4.7	5.3	5.9
Average Estimate (10% Growth in Data Per Year)	2.7	3.0	3.3	3.6	3.9	4.3	4.8	5.2
Conservative Estimate(8% Growth in Data Per Year)	2.7	2.9	3.1	3.4	3.7	4.0	4.3	4.6

i) Server Load Estimation

Assumptions:

Total No. of users for the solution = 1000 (Approx.)

Maximum No. of concurrent users (15% of 1000) = 150

Percentage of light weight users: 70%

Percentage of medium weight users: 20%

Percentage of heavy users: 10%

User Category	Maximum No. of concurrent users	Average No. of transactions per day per user	Average Band width requirement per user	Load
Light	105	15	1 KBPS	1.575 MBPS
Medium	30	25	3 KBPS	2.25 MBPS
Heavy	15	20	10 KBPS	3.0 MBPS

Additional bandwidth requirements for email, other data intensive operations etc. will be another 1 Mbps

An additional 0.5 Mbps should be kept as a reserve buffer to handle any surge of requests as well as special data intensive processing in an one off mode

Based on the above observations, it is envisaged that a bandwidth requirement of approximately 8.325 MBPS.

D. CDC and DR Specification

This section elaborates the technical and infrastructure specifications for the CDC and DR site at IRDA

Hardware Specifications

It is recommended to design a hardware infrastructure that will not only address the present requirements of the IRDA application but will also take into account the future high-bandwidth and high availability of the application stack. Hardware infrastructure should have:

- High Availability: Application, Web and database servers have been designed in failover and firm mode with an ability to ensure full-proof operations
- Separate Storage: Additional space requirements for IRDA in future will ensured through a separate Storage Area Network (SAN) driven disk. The disk will also be mirrored to ensure data protection and integrity
- Redundancy: Adequate processing and capacity redundancy have been built in within the system to ensure zero to minimal disruption in the overall operations

Table below describes various hardware components envisaged for the solution in the main data center:

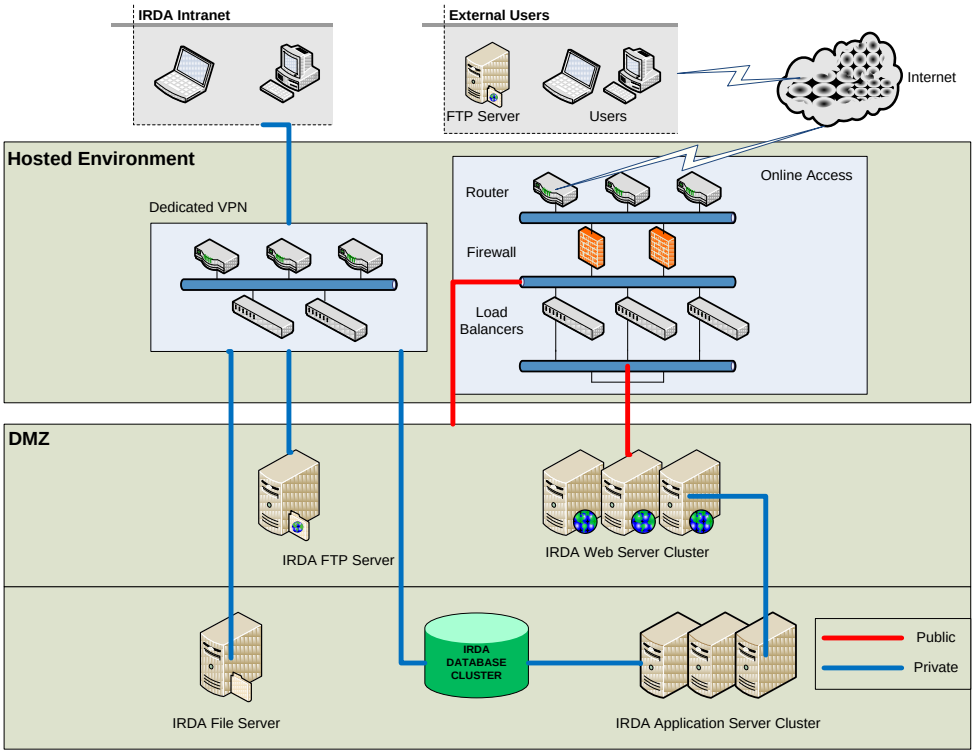
Components	Specification	Comments
Web Server	2 Processors with dual core each or higher	Configured in a cluster of 2. May use existing hardware and infrastructure
Web Accelerator/Load Balancer	6 Processors with quad core each	Configured in a cluster of 2. May use existing hardware and infrastructure
Database Server	6 Processors with quad core each	Configured in a cluster of 2. May use existing hardware and infrastructure
Application Server	6 Processors with quad core each	Configured in a cluster of 2. May use existing hardware and infrastructure
Web Services Server	2 Processors with dual core each or higher	Configured in a cluster of 2. May use existing hardware and infrastructure
Firewall/Proxy Gateway	2 Processors with dual core each or higher	Existing firewall and gateway may be used
Storage Device	Capacity of around 5 TB with	Additional storage capacity

Components	Specification	Comments
	RAID 10 disk mirroring configuration	available may be leveraged
Routers	Standard with 2 c v.35 port and 1 x ISDN failover	1 router planned.; but any existing capacity will be reused
Switches	Switch 24 port 10/100/1000 mbps Switch - (Catalyst 2960 24 10/100/1000, 4 T/SFP)	1 Switch planned; but any existing capacity will be reused
Firewall	4 x 10/100/1000 ports Firewall	Firewall in High Availability mode should be used. Existing set-up may be re-used
Modems	Standard configuration modem with failover	Existing set-up may be re-used

All components of the proposed infrastructure should be configured in a fail over mode. This will ensure no single point of failure of the system and a high availability of the application for its end users. To optimize performance, load balancing should be implemented using a group of web servers. No antivirus software envisaged in the facility as it will be configured through high-end firewall configurations. Desktops will be protected using standard antivirus software

Network Specifications

Networking will be enabled by two virtualized ports configured in a failover mode. Dedicated VPN links will be established between Development environment and Hosted Services environment for development purposes.



Application design will ensure that all the data intensive processing will be restricted as back-end server process within the data centre environment. Data centre will operate on a dedicated 10/100 MBPS LAN ensuring the processing integrity. All the master data managed facilities; application intensive processing as well as transactions will be carried out through the standard internet traffic from the field.

Physical Infrastructure Specifications

Civil Interiors

Around 250 square foot of facilities should be made available at a designated area at IRDA. The room should have four walls and a ceiling with an appropriate clearance for putting server racks. Following sections details out an indicative approach to the different facets of the data centre design, securities and maintenance operations.

Civil and Masonry

Following civil and masonry work will be conducted as part of the operations. If the current facilities have the features available according to the specification, minor alterations may be carried out on the same

- 9-inch thick brick wall will be laid to ensure safety and compliance standards
- Walls will be all plastered
- A ramp will be provided at the entrance. Laying and fabrication work of the ramp will be carried out according to the required slope angle specification.
- Good penetrations will be made on all doors and seals with appropriate fire-stop material to ensure integrity
- Anti-termite treatment will be provided initially as well as on periodic basis

Joinery

- Main fire door will be a 2.4 m double winged , fire rated 1.5 x 2.4 m , double door with 300x900 mm fire rated flass vision panel
- 100 mm x 50 mm marandi/equivalent wooden frame fire glass will be provided with Fire Check material in the top and bottom along with minimum 6 mm thick 1 hour Fire rated glass with beading and finished with approved colors of 1.5 mm thick
- FULL HEIGHT CALCIUM SILICATE (FIRE RATE MIN 1 Hour) BOARD PARTITION will be provided for fire control. Calcium Silicate board partition (Non Asbestos) faced both sides will be 12 mm thick. Skirting, door junction and material transition sections to be in hardwood frame 50 x to provide 10x10 grooves at all ends. If any hardwood sections are provided, these are to be coated all over with 2 or more coats of viper anti-termite/fire retard paint. Inside voids to be filled with 50 mm thick panels of glass wool/ rock wool. All board edges to be protected with aluminium angles

Access Flooring and Insulation Work

- ACCESS FLOOR: Adjusting floor panels of 450+/- 20mm height will be provided under floor construction
- Self adhesive type 13mm thick XLPE foam on under deck & floor including metalized foil complete with proper jointing will be provided as insulation

False Ceiling

- Armstrong or equivalent make false ceiling including making openings for electrical light fitting complete and fire alarm detectors and nozzles will be provided

Painting and Epoxy Works

- Plastic/acrylic light textured emulsion paint will be applied on server room internal walls. Epoxy coating will be applied to the Duco paint will be provided for fire decor

Additionally appropriate fire and security signage will be provided as well

Electrical Works & Cabling and Racks

- 6 amp outlets with universal pin along with MS Box will be installed
- Wiring for 16 amp power outlet points with 4 sq. mm PVC insulated copper conductor wire will be installed for hardware
- Supplying and fixing of 63 amp 5-pin (Three phase Neutral and earth) for 3-phase industrial socket outlet will be provided for
- Cat6 UTP Cable, roll of 305m will be used for cabling
- 19" Rack 42U/800W/1000D Aluminium Extruded Structure (For Safe Working Load of 1000Kgs) with Side Panels with Top and Bottom panel will be provided for housing the server and Storage devices

Access Control System

Data Centre will have access control system with proximity card reader with appropriate security control procedures established. Standard features for such a system is outlined below:

- 1 Door Control Unit for Access Control, microprocessor based with tamper protected wall-mount case
- Low power 12 V DC power supply with internal battery backup for 4 hours operation.
- Proximity card Readers with 3" read range capable of
  - ✓ Reading the facility code and unique card number from the card
  - ✓ Shall only read the card data and passes on to the door controller for validation
- ISO thickness Proximity Cards (Blank faced) with option of printing directly on card. Card has facility code, and unique card number
- Electromagnetic Locks (600 lbs) with Magnetic Contact UL listed for single leaf doors
- Emergency Door Release (Break Glass Type)
- 1:N authentication Biometric Finger Print Reader with inbuilt proximity reader
- Access Management Software complete with Graphic User Interface, Time & Attendance software – transactions, Anti-passback features complete as required

Fire Detection System

Standard fire extinguishers will be deployed in the server room

Air Conditioning

3 TR capacity PeX135FA-100 Precision AC, Floor discharge type with R-407C with Ethernet Connectivity and Sequential controller will be provided with appropriate climate control features

Power Back-up

Power back-up is an important feature to protect the facility from outage. Following UPS features will be available in the data centre

- Liebert make 7400M 30/40 KVA UPS system with 3 phase input and 3 phase output with accessories
- Sealed Maintenance free Battery to Support approximately 30 minutes back-up

Additionally a standard public address system as well as a Rodent insect repellent should also need to be installed in the data centre.

Service Level for the proposed Data Center

Since most of the services to be provided by Data Center (DC) are highly critical to IRDA, the efficiency of DC operation should be of high importance. The service levels should be of prime importance to ensure high efficiency of DC operations. The proposed technical architecture requires high availability .This should be achieved through a High Available Design at various IT Infrastructure layers.

Along with the design, there is a need for strong IT infrastructure management processes and a comprehensive maintenance plan involving maintenance engineers, spares and backend support from OEMs for spare replenishment.

The key considerations for ensuring high efficiency of Data Center (DC) operations are discussed in the table below:

Operations	Should be 24 x 7 x 365
Computing, Storage and Application Environment	From an operational perspective, the system should provide enough availability to give comfort to applicants in terms of reliability and efficiency of the system. Service Level for ensuring uptime should be 99.9 per cent The architecture should have 'No Single Point Of Failures'
Communication Network	The MPLS backbone and Network should have assured uptime and therefore two separate links from two individual service providers should be used. Service Level for ensuring uptime should be 99.9 per cent
Information Security	Information Security at various layers prohibiting the possible security threats should be ensured. Security should be ensured for the application data, Network and Physical Infrastructure being set up under this project. Security threats from unknown networks integrating with IRDA such as Insurer need special attention and the design should take care of such users in a different manner.

Power	Adequate power backups to prevent system downtime
Maintainability	Adequate spares at the sites for all elements with single point of failure, sufficient on-site manpower to failure resolution on site, and back-to-back spare replenishment plan with minimum spares turnaround time from the Product OEMs should be ensured.
Manageability	Latest tools for Incident Management including Help desk, Problem Management and Asset Management should be used and appropriate processes should be defined based on the ITIL framework.

E. Technical details of Security for IRDA Business Analytics Solution

Application Tier

This is the innermost security tier covering the security aspects of the applications running in IRDA setup. This application tier should have following security aspects:

Identification and Authentication – Multi Factor Authentication

Two-factor, or multi-factor authentication is exactly what it sounds like. Instead of using only one type of authentication factor, such as only things a user KNOWS (login IDs, passwords, secret images, shared secrets, solicited personal information, etc), two-factor authentication requires the addition of a second factor, the addition of something the user HAS or something the user IS. For IRDA there is need for such multi factor authentications, especially for sensitive data like product pricing etc.

Two-factor authentication is a commonly used concept. For example, the two-factor authentication is used every time a bank customer visits their local ATM machine. One authentication factor is the physical ATM card the customer slides into the machine. The second factor is the PIN they enter. Without both, authentication cannot take place. This scenario illustrates the basic parts of most multi-factor authentication systems; the "something you have" + "something you know" concept.

Types of Multi Factor Authentication are given below:

Tokens

One form of 'something you have' is the smart card and USB tokens. Differences between the smart card and USB token are diminishing; both technologies include a microcontroller, an OS, a security application, and a secured storage area.

Virtual Tokens

Virtual tokens are a new concept in multi-factor authentication first introduced in 2005 by security company, Sestus. Virtual tokens reduce the costs normally associated with implementation and maintenance of multi-factor solutions by utilizing the user's existing internet device as the "something the user has" factor. Also, since the user's internet device is communicating directly with the authenticating website, the solution does not suffer from man-in-the-middle attacks and other forms of online fraud.

Biometrics

Biometric authentication also satisfies the regulatory definition of true multi-factor authentication. Users may biometrically authenticate via their fingerprint, voiceprint, or iris scan using provided hardware and then enter a PIN or password in order to open the credential vault. However, while this type of authentication is suitable in limited applications, this solution may become unacceptably slow

and comparatively expensive when a large number of users are involved. In addition, it is extremely vulnerable to a replay attack: once the biometric information is compromised, it may easily be replayed unless the reader is completely secure and guarded. Finally, there is great user resistance to biometric authentication. Users resist having their personal physical characteristics captured and recorded for authentication purposes.

For many biometric identifiers, the actual biometric information is rendered into string or mathematic information. The device scans the physical characteristic, extracts critical information, and then stores the result as a string of data. Comparison is therefore made between two data strings, and if there is sufficient commonality a pass is achieved. It may be appreciated that choice of how much data to match, and to what degree of accuracy, governs the accuracy/speed ratio of the biometric device. All biometric devices, therefore, do not provide unambiguous guarantees of identity, but rather probabilities and all may provide false positive and negative outputs. If a biometric system is applied to a large number of users - perhaps all of the customers of a bank, the error rate may make the system impractical to use.

Biometric information may be mechanically copied and they cannot be easily changed. This is perceived as a key disadvantage since, if discovered, the compromised data cannot be changed. A user can easily change his/her password; however, a user cannot change their fingerprint. A bio-identifier can also be faked. For example, fingerprints can be captured on sticky tape and false gelatine copies made, or simple photos of eye retinas can be presented. More expensive biometrics sensors should be capable to distinguish between live original and dead replicas, but such devices are not practical for mass distribution. It is likely that, as biometric identifiers become widespread, more sophisticated compromise techniques will also be developed.

Historically, fingerprints have been used as the most authoritative method of authentication. Other biometric methods such as retinal scans are promising, but have shown themselves to be easily spoofable in practice. Hybrid or two-tiered authentication methods offer a compelling solution, such as private keys encrypted by fingerprint inside of a USB device.

SMS One Time Password

SMS One time password uses information sent as an SMS to the user as part of the login process. One scenario is where a user either registers (or updates) their contact information on a website. During this time the user is also asked to enter his or her regularly used telephone numbers (home, mobile, work, etc). The next time the user logs in to the website, they must enter their username and password; if they enter the correct information, the user then chooses the phone number at which they can be contacted immediately from their previously registered phone numbers. The user will be instantly called or receive an SMS text message with a unique, temporary PIN code. The user then enters this code into the website to prove their identity, and if the PIN code entered is correct, the user will be granted access to their account. This process provides an extra layer of online security beyond merely a username and password. These solutions can be used with any telephone, not just mobile devices.

There is a newer method of using the mobile phone as the processor and having the Security Token reside on the mobile as a Java ME client. This method does not include data latency or incur hidden costs for the end user. While such methods can simplify deployment, reduce logistical costs, and remove the need for a separate hardware token devices, there are numerous trade-offs. Users may incur fees for text/data services or cellular calling minutes. In addition, there is a latency involved with SMS services especially during peak SMS usage periods like the holidays. Finally, as with telephone-based processes, these processes are also vulnerable to man-in-the-middle attacks. The victim visits a counterfeit website where they supply their login credentials. The counterfeit website passes these to the legitimate website using scripts or other protocols. The legitimate website initiates an SMS text message delivery of a one-time-password to the victim's mobile device or simply waits for the Java token value to be generated. The victim enters the one-time-password onto the counterfeit website, which then forwards this to the legitimate website, where the waiting fraudster uses it to complete their access.

Universal Serial Bus

A USB token has different form factor; it can't fit in a wallet, but can easily be attached to a key ring. A USB port is standard equipment on today's computers, and USB tokens generally have a much larger storage capacity for logon credentials than smart cards. As with smart cards, magnetic card readers, and mobile signature methods, they are costly to deploy and support, are vulnerable to numerous forms of theft and fraud, and have been resisted by consumers.

Digital Certificates

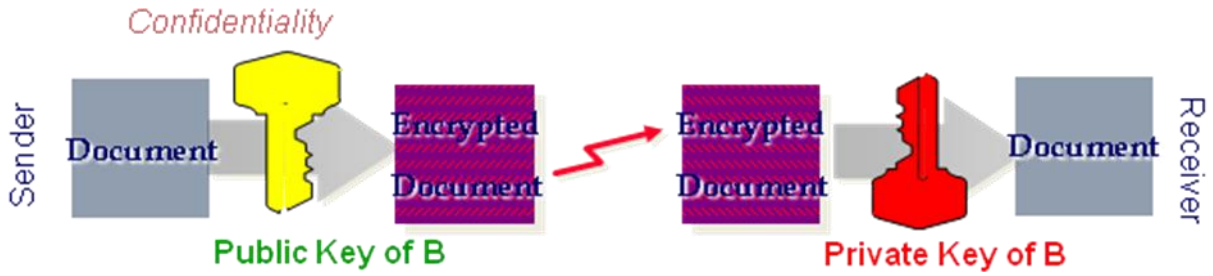
Digital Client certificates are PKI solutions for enabling the enhanced user identification and access controls needed to protect sensitive online information. Digital certificates can also be stored and transported on smart cards or USB tokens for use when travelling. Each certificate can only be used to authenticate one particular user because only that user’s computer has the corresponding and unique private key needed to complete the authentication process. Client certificates are delivered electronically; however, deployment and support of digital certificates have proven problematic. In a 2008 study published by the Credit Union Journal, digital certificates were noted as averaging very high support costs and very low rates of user acceptance due to difficult technical implementation requirements.

Identification and Authentication – Digital Signature

Converting the paper based data capture process to online data submission will require utilizing some advanced data authentications mechanism like Digital Signature. For quite a few returns submitted by Insurer require physical signoff by various stakeholders like CFO, Auditor, Appointed Actuary etc. This section will focus on various aspects of Digital Signature for utilizing it appropriately at IRDA.

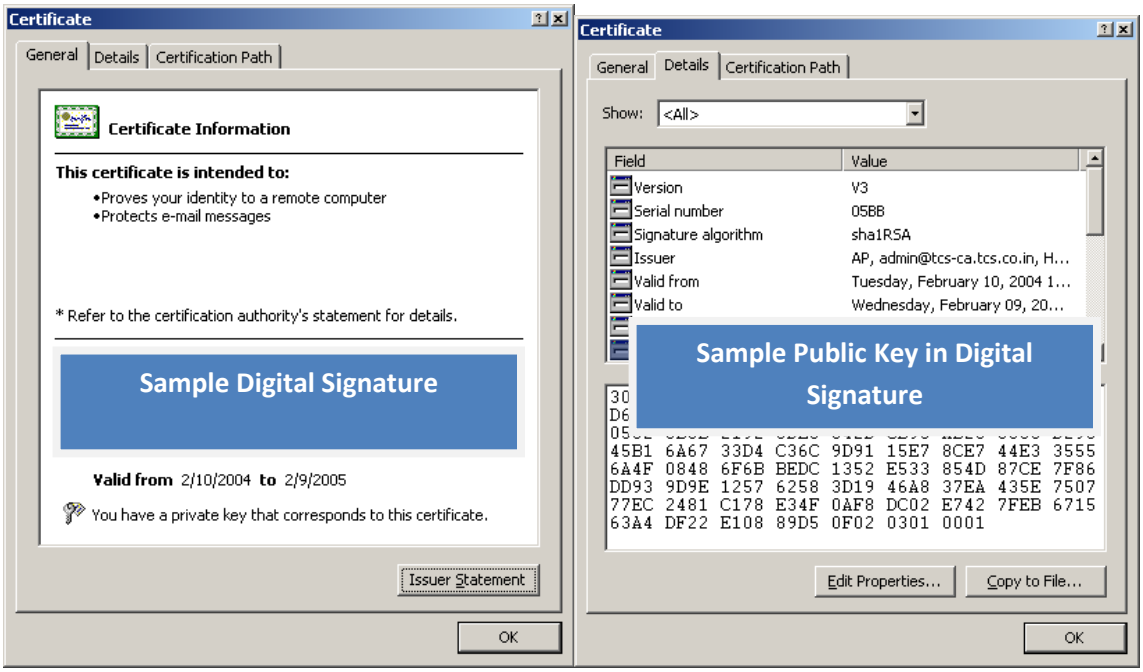
The Information Technology Act, 2000 provides for use of Digital Signatures on the documents submitted in electronic form in order to ensure the security and authenticity of the documents filed electronically. This is the only secure and authentic way that a document can be submitted

electronically. As such, all filings done by the companies under MCA21 e-Governance programme are required to be filed with the use of Digital Signatures by the person authorized to sign the documents.

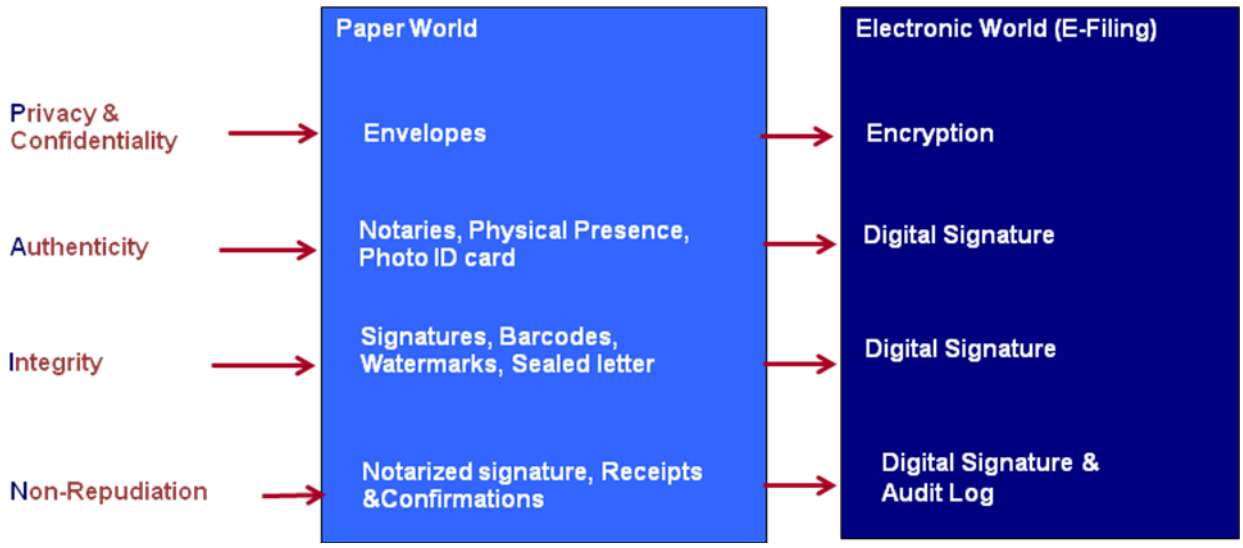


Digital Signature provides the following:

- Authentication/ Identification (Who)
- Message Integrity (What)
- Non Repudiation/Non Denial (Legal Binding)



Digital Signature is used in Electronic filing or e-filing which is a method of filing signed document that uses an electronic format rather than a traditional paper format. Parties convert their documents into the file format designated by the authority and file their documents via email or over the Internet. Scenario comparison between Digital Signature and traditional authentication is given below:



Advantage of Digital Signature:

- Transactions can be done electronically with a click of a button.
- Details are sent across instantaneously once the information is submitted. No time delay in communication.
- Processing & approval done electronically at each level and hence takes less time
- All the official communications can be sent through email, which is fast and cost-effective
- Ensures PAIN (Privacy & Confidentiality, Authenticity, Integrity, Non-Repudiation)
- Archival of information is possible. Also retrieval of the archived data is easier
- No physical storage is required for the documents
- Legal sanctity in a court of law

Process for using Digital Signature

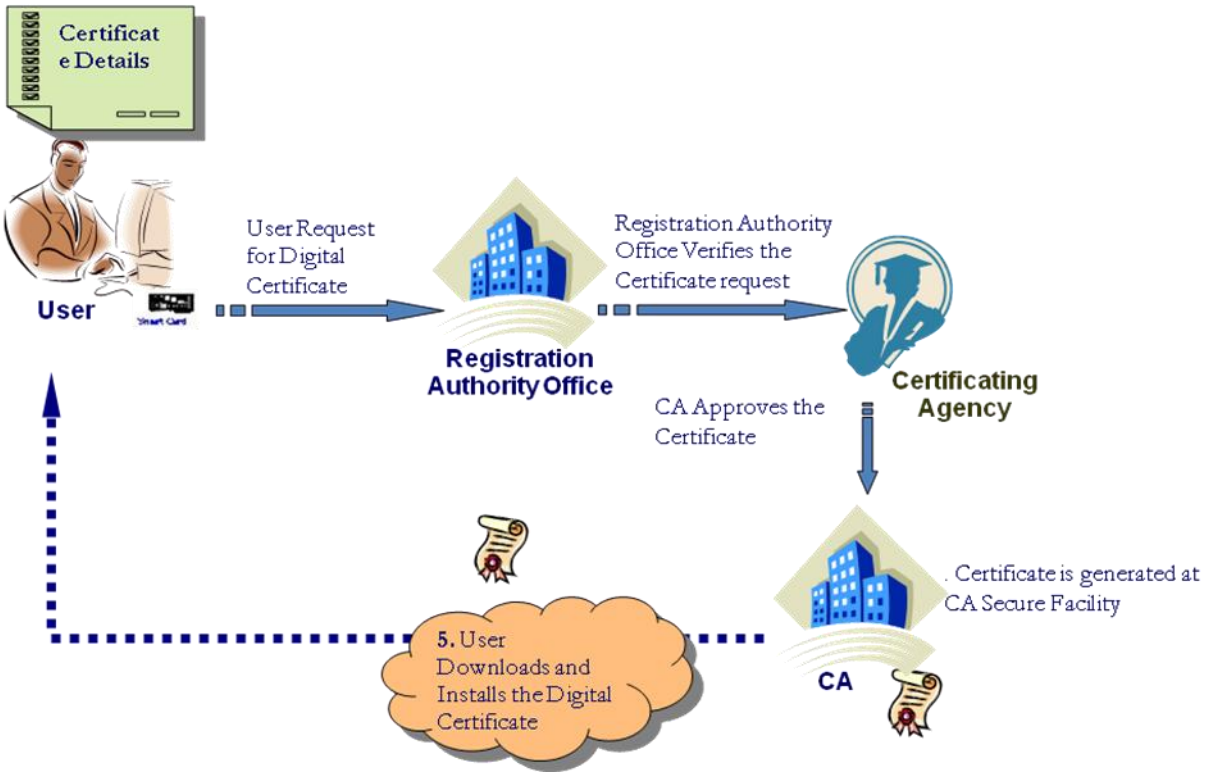
- Getting a Private and Public Key: In order to electronically sign documents with standard digital signatures, sender needs to obtain a Private and Public Key – a one-time setup/operation. The Private Key, as the name implies, is not shared and is used only by the signer to sign documents. The Public Key is openly available and used by those that need to validate the signer's digital signature.
- Initiate the signing process: Depending on the software used, sender needs to initiate the signing process (e.g. clicking a "Sign" button on the software's toolbar).
- Create a digital signature: A unique digital fingerprint of the document (sometimes called Message Digest or Document Hash) is created using a mathematical algorithm (such as SHA-1). Even the slightest difference between two documents would create a different digital fingerprint of the document.
- Append the signature to the document: The hash result and the user's digital certificate (which includes his Public Key) are combined into a digital signature (by using the user's Private Key to

encrypt the document hash). The resulting signature is unique to both the document and the user. Finally, the digital signature is appended to the document.

- Initiates the validation process: depending on the software used, the receiver needs to initiate the signing process (e.g. clicking a “Validate Signature” menu option button on the software’s toolbar).
- Decrypts Sender’s signature: Using his Public Key and gets the original document (the document fingerprint).
- Compare Senders fingerprint with calculated: Software then calculates the document hash of the received document and compares it with the original document hash (from the previous step). If they are the same, the signed document has not been altered.

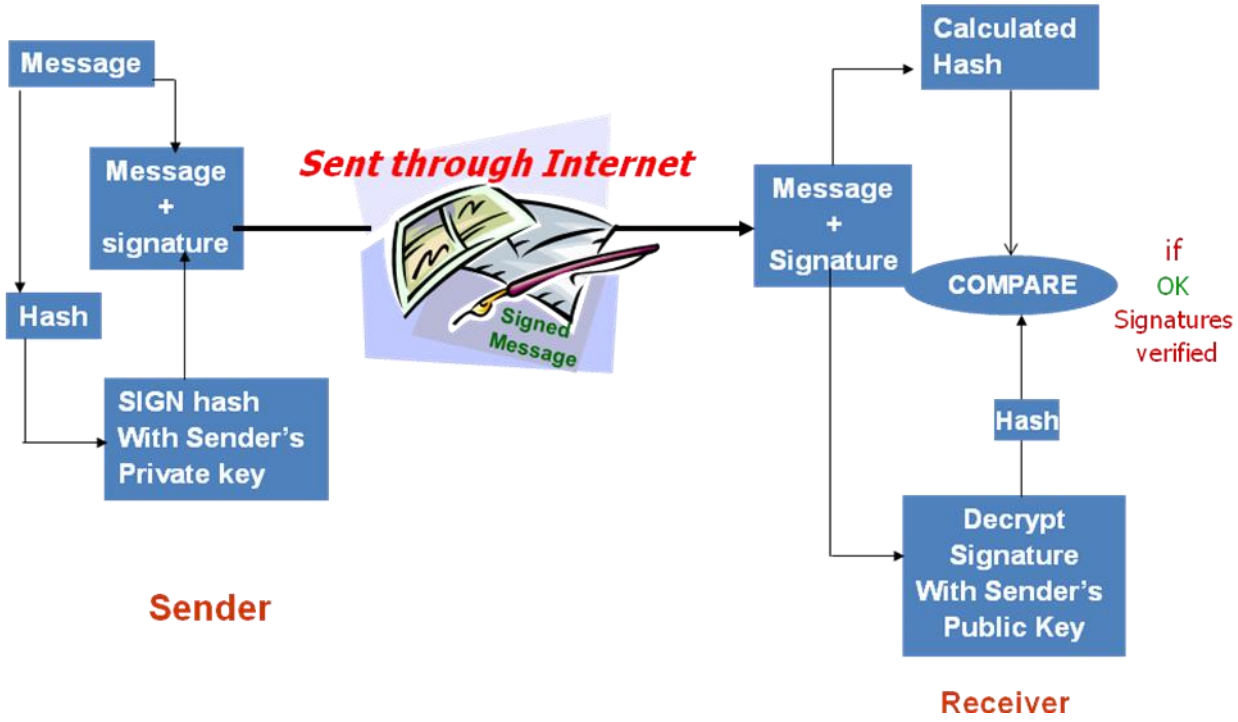
Proposed Process flow of acquiring Digital Signature

Based on the specific data confidentiality requirement at IRDA, the following process flow is proposed for acquiring Digital Signature:



Proposed process flow of validating Digital Signature

Based on the specific data confidentiality requirement at IRDA, the following process flow is proposed for validating Digital Signature:



Access Control – Role Based Access

Within IRDA, roles are created for various job functions. The permissions to perform certain operations are assigned to specific roles. Members of staff (or other system users) are assigned particular roles, and through those role assignments acquire the permissions to perform particular system functions. Unlike context-based access control (CBAC), RBAC does not look at the message context (such as a connection's source).

Since users are not assigned permissions directly, but only acquire them through their role (or roles), management of individual user rights becomes a matter of simply assigning appropriate roles to the user; this simplifies common operations, such as adding a user, or changing a user's department.

RBAC differs from access control lists (ACLs) used in traditional discretionary access control systems in that it assigns permissions to specific operations with meaning in the organization, rather than to low level data objects. For example, an access control list could be used to grant or deny write access to a particular system file, but it would not dictate how that file could be changed. In an RBAC-based system, an operation might be to create a 'credit account' transaction in a financial application or to populate a 'blood sugar level test' record in a medical application. The assignment of permission to perform a

particular operation is meaningful, because the operations are granular with meaning within the application. RBAC has been shown to be particularly well suited to separation of duties (SoD) requirements, which ensure that two or more people must be involved in authorizing critical operations. Necessary and sufficient conditions for safety of SoD in RBAC have been analyzed. An underlying principle of SoD is that no individual should be able to affect a breach of security through dual privilege. By extension, no person may hold a role that exercises audit, control or review authority over another, concurrently held role.

Audit and Accountability – Audit Logging

Audit log is a chronological sequence of audit records, each of which contains evidence directly pertaining to and resulting from the execution of a business process or system function.

Audit Trails provides track, trace and reporting capabilities for any changes associated with any data a system, and for any data in third-party software or customized software resident

System & Communications Protection – SSL

Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols that provide security for communications over networks such as the Internet. TLS and SSL encrypt the segments of network connections at the Transport Layer end-to-end.

In applications design, TLS is usually implemented on top of any of the Transport Layer protocols, encapsulating the application specific protocols such as HTTP, FTP, SMTP, NNTP, and XMPP. Historically it has been used primarily with reliable transport protocols such as the Transmission Control Protocol (TCP). However, it has also been implemented with datagram-oriented transport protocols, such as the User Datagram Protocol (UDP) and the Datagram Congestion Control Protocol (DCCP), usage which has been standardized independently using the term Datagram Transport Layer Security (DTLS).

A prominent use of TLS is for securing World Wide Web traffic carried by HTTP to form HTTPS. Notable applications are electronic commerce and asset management. Increasingly, the Simple Mail Transfer Protocol (SMTP) is also protected by TLS (RFC 3207). These applications use public key certificates to verify the identity of endpoints.

An increasing number of client and server products support TLS natively, but many still lack support. As an alternative, users may wish to use standalone TLS products like Stunnel. Wrappers such as Stunnel rely on being able to obtain a TLS connection immediately, by simply connecting to a separate port reserved for the purpose.

TLS can also be used to tunnel an entire network stack to create a VPN, as is the case with OpenVPN. Many vendors now marry TLS's encryption and authentication capabilities with authorization. When compared against traditional IPsec VPN technologies, TLS has some inherent advantages in firewall and NAT traversal that make it easier to administer for large remote-access populations.

TLS is also a standard method to protect Session Initiation Protocol (SIP) application signalling. TLS can be used to provide authentication and encryption of the SIP signalling associated with VoIP and other SIP-based applications.

System & Communications Protection – Data Encryption

In cryptography, encryption is the process of transforming information (referred to as plaintext) using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. The result of the process is encrypted information (in cryptography, referred to as ciphertext). In many contexts, the word encryption also implicitly refers to the reverse process, decryption (e.g. "software for encryption" can typically also perform decryption), to make the encrypted information readable again (i.e. to make it unencrypted).

System Tier

It is a branch of technology known as information security as applied to computers and networks. The objective of system security includes protection of information and property from theft, corruption, or natural disaster, while allowing the information and property to remain accessible and productive to its intended users. The term system security means the collective processes and mechanisms by which sensitive and valuable information and services are protected from publication, tampering or collapse by unauthorized activities or untrustworthy individuals and unplanned events.

Systems & Information Integrity – Software Integrity

System integrity means:

- That condition of a system wherein its mandated operational and technical parameters are within the prescribed limits.
- The quality of an Automated Information System when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.
- The state that exists when there is complete assurance that under all conditions an IT system is based on the logical correctness and reliability of the operating system, the logical completeness of the hardware and software that implement the protection mechanisms, and data integrity.

Data integrity is a term used in computer science and telecommunications that can mean ensuring data is "whole" or complete, the condition in which data is identically maintained during any operation (such as transfer, storage or retrieval), the preservation of data for their intended use, or, relative to specified operations, the a priori expectation of data quality. Put simply, data integrity is the assurance that data is consistent and correct.

In terms of a database data integrity refers to the process of ensuring that a database remains an accurate reflection of the universe of discourse it is modelling or representing. In other words there is a close correspondence between the facts stored in the database and the real world it models

Identification & Authentication – Strong Passwords

Identification is the process by which the identity of a user is established, and authentication is the process by which a service confirms the claim of a user to use a specific identity by the use of credentials (usually a password or a certificate).

Identification is an assertion of who someone is or what something is. If a person makes the statement "Hello, my name is John Doe." they are making a claim of who they are. However, their claim may or may not be true. Before John Doe can be granted access to protected information it will be necessary to verify that the person claiming to be John Doe really is John Doe.

Authentication is the act of verifying a claim of identity. When John Doe goes into a bank to make a withdrawal, he tells the bank teller he is John Doe (a claim of identity). The bank teller asks to see a photo ID, so he hands the teller his driver's license. The bank teller checks the license to make sure it has

John Doe printed on it and compares the photograph on the license against the person claiming to be John Doe. If the photo and name match the person, then the teller has authenticated that John Doe is who he claimed to be.

There are three different types of information that can be used for authentication: something you know, something you have, or something you are. Examples of something you know include such things as a PIN, a password, or your mother's maiden name. Examples of something you have include a driver's license or a magnetic swipe card. Something you are refers to biometrics. Examples of biometrics include palm prints, finger prints, voice prints and retina (eye) scans.

Using strong passwords lowers overall risk of a security breach, but strong passwords do not replace the need for other effective security controls. The effectiveness of a password of a given strength is strongly determined by the design and implementation of the authentication system software, particularly how frequently password guesses can be tested by an attacker and how securely information on user passwords is stored and transmitted.

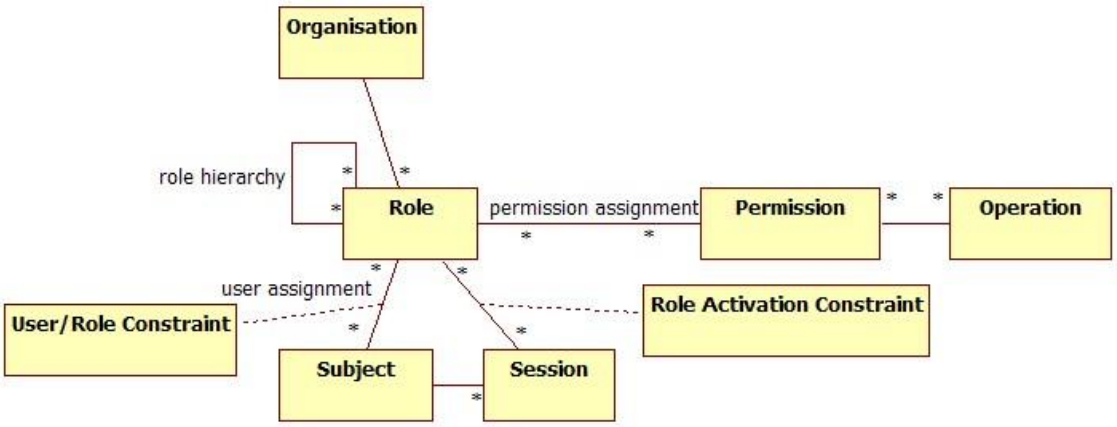
Access Control – Role Bases Access

Access to protected information must be restricted to people who are authorized to access the information. The computer programs, and in many cases the computers that process the information, must also be authorized. This requires that mechanisms be in place to control the access to protected information. The sophistication of the access control mechanisms should be in parity with the value of the information being protected - the more sensitive or valuable the information the stronger the control mechanisms need to be. The foundation on which access control mechanisms are built, start with identification and authentication.

Role-based access control (RBAC) is an approach to restricting system access to authorized users. It is a newer alternative approach to mandatory access control (MAC) and discretionary access control (DAC). RBAC is sometimes referred to as role-based security.

RBAC is a policy neutral and flexible access control technology sufficiently powerful to simulate DAC and MAC.

With the concepts of role hierarchy and constraints, one can control RBAC to create or simulate lattice-based access control (LBAC). Thus RBAC can be considered a superset of LBAC.



Audit & Accountability – Audit Logging

Audit trail or audit log is a chronological sequence of audit records, each of which contains evidence directly pertaining to and resulting from the execution of a business process or system function.

Audit records typically result from activities such as transactions or communications by individual people, systems, accounts or other entities. The process that creates audit trail should always run in a privileged mode, so it could access and supervise all actions from all users, and normal user could not stop/change it. Furthermore, for the same reason, trail file or database table with a trail should not be accessible to normal users.

Accountability uses such system components as audit trails (records) and logs to associate a subject with its actions. The information recorded should be sufficient to map the subject to a controlling user. Audit trails and logs are important for

- Detecting security violations
- Re-creating security incidents

If no one is regularly reviewing your logs and they are not maintained in a secure and consistent manner, they may not be admissible as evidence.

Many systems can generate automated reports based on certain predefined criteria or thresholds, known as clipping levels. For example, a clipping level may be set to generate a report for the following:

- More than three failed logon attempts in a given period
- Any attempt to use a disabled user account

These reports help a system administrator or security administrator to more easily identify possible break-in attempts.

System & Communications protection

When organizations think of backup and recovery, it is usually associated with protecting information residing on a server. It is important in IRDA's context to remember, however, that this constitutes both

data and system information. Too often, so much emphasis is put on the need to protect the data that the system is overlooked. But if the system is not operable, the chances of accessing the data are slim.

When a server operating system fails, it can take eight or more hours (days, in some instances) to rebuild and restore the server. This process includes reinstalling the OS, applications, patches, configuring settings, etc. Moreover, there are no guarantees that the server will be in the exact same state as before the failure took place.

There is also the matter of having to replace the server hardware. Few organizations can afford the luxury of maintaining extra server hardware in case they need to replace an existing system. This introduces the issue of restoring a system to a new and dissimilar piece of hardware, while trying to preserve the integrity of the system state and the availability of the data. Organizations must ensure that their system backup/recovery solutions provide hardware-independent restoration.

By deploying both data protection and system recovery solutions, organizations of any size can realize the benefits of shorter backup times, faster system recovery, and reduced data loss.

For this purpose it is recommended to use Disaster Recovery Site for IRDA to protect the Data and Applications considering the sensitivity and criticality of the data that IRDA deals with.

Network Tier

Network security consists of the provisions made in an underlying computer network infrastructure, policies adopted by the network administrator to protect the network and the network-accessible resources from unauthorized access, and consistent and continuous monitoring and measurement of its effectiveness (or lack) combined together.

Network security starts from authenticating the user, commonly with a username and a password. Since this requires just one thing besides the user name, i.e. the password which is something you 'know', this is sometimes termed one factor authentication. With two factor authentication something you 'have' is also used (e.g. a security token or 'dongle', an ATM card, or your mobile phone), or with three factor authentication something you 'are' is also used (e.g. a fingerprint or retinal scan).

Once authenticated, a firewall enforces access policies such as what services are allowed to be accessed by the network users. Though effective to prevent unauthorized access, this component may fail to check potentially harmful content such as computer worms or Trojans being transmitted over the network. Anti-virus software or an intrusion prevention system (IPS) helps to detect and inhibit the action of such malware. An anomaly-based intrusion detection system may also monitor the network and traffic for unexpected (i.e. suspicious) content or behaviour and other anomalies to protect resources, e.g. from denial of service attacks or an employee accessing files at strange times. Individual events occurring on the network may be logged for audit purposes and for later high level analysis.

Security management

It is recommended to have following Network security measurements for the IRDA system.

- A strong firewall and proxy to keep unwanted people out.
- A strong Antivirus software package and Internet Security Software package.
- For authentication, use strong passwords and change it on a weekly/bi-weekly basis.
- When using a wireless connection, use a robust password.
- Exercise physical security precautions to employees.
- Prepare a network analyzer or network monitor and use it when needed.
- Implement physical security management like closed circuit television for entry areas and restricted zones.
- Security fencing to mark the company's perimeter.
- Fire extinguishers for fire-sensitive areas like server rooms and security rooms.
- Security guards can help to maximize security.

It is also recommended for IRDA to design and implement a IT Security policy to safeguard its IT assets. Everything that is done in the name of security, then, must enforce that policy uniformly. The following part of this section focuses on the Network Security components.

Firewalls

In order to provide some level of separation between IRDA's intranet and the Internet, firewalls would have to be employed. A firewall is simply a group of components that collectively form a barrier between two networks.

Few terms related to firewalls:

Bastion host

A general-purpose computer used to control access between the internal (private) network (intranet) and the Internet (or any other un-trusted network). Typically, these are hosts running a flavour of the Unix operating system that has been customized in order to reduce its functionality to only what is necessary in order to support its functions. Many of the general-purpose features have been turned off, and in many cases, completely removed, in order to improve the security of the machine.

Router

A special purpose computer for connecting networks together. Routers also handle certain functions, such as routing, or managing the traffic on the networks they connect.

Access Control List (ACL).

Many routers now have the ability to selectively perform their duties, based on a number of facts about a packet that comes to it. This includes things like origination address, destination address, destination

service port, and so on. These can be employed to limit the sorts of packets that are allowed to come in and go out of a given network.

Demilitarized Zone (DMZ)

The DMZ is a critical part of a firewall: it is a network that is neither part of the untrusted network, nor part of the trusted network. But, this is a network that connects the untrusted to the trusted. The importance of a DMZ is tremendous: someone who breaks into your network from the Internet should have to get through several layers in order to successfully do so. Those layers are provided by various components within the DMZ.

Proxy

This is the process of having one host act in behalf of another. A host that has the ability to fetch documents from the Internet might be configured as a proxy server, and host on the intranet might be configured to be proxy clients. In this situation, when a host on the intranet wishes to fetch the IRDA's web page, for example, the browser will make a connection to the proxy server, and request the given URL. The proxy server will fetch the document, and return the result to the client. In this way, all hosts on the intranet are able to access resources on the Internet without having the ability to direct talk to the Internet.

F. Security Settings for IRDA Business Analytics Project

The following section outlines the various application components that are used to administer security. This strategy includes the decisions IRDA has made regarding the processing options settings for the security objects.

1) Sign-On Security

#	Description	Possible Value(s)	IRDA BAP Settings
1	Unique ID generation	• 1 – Enable Default • Blank – Disable	Blank – Detail a complex initial password for new User IDs
2	Maximum number of days before the system requires a password change.	11 digits are possible: (Range of: 0 – 99999999999)	Password Change Frequency: 45 Days
3	The number of times that a user can unsuccessfully attempt to log on before his or her account is disabled.	3 digits are possible: (Range of: 0 – 999)	Unsuccessful Logon Attempts Before Account Lock-out: 3
4	Indicates if the user's account is enabled or disabled. A disabled account is not allowed into the business analytics solution	• 01 - Enable • 02 - Disable	Enable
5	Force immediate password change for new users	• 0 – No • 1 - Yes	Yes
6	The number of times that a user can change his or her password in one day.	10 digits are possible (Range of 0 – 9999999999)	3

#	Description	Possible Value(s)	IRDA BAP Settings
7	Minimum password length	5 digits (Range of: 0 – 99999)	8
8	Minimum number of characters to be used in the password	5 digits (Range of: 0 – 99999)	1
9	Minimum number of characters to be used in the password	5 digits (Range of: 0 – 99999)	1
10	Maximum number of consecutive characters in the password	5 digits (Range of: 0 – 99999)	0
11	Minimum number of special characters required in the password	5 digits (Range of: 0 – 99999)	0

In addition, the following global password settings will be configured, in accordance with IRDA's requirements. The

Setting	IRDA BAP Settings
Minimum password length	8
Minimum number of characters to be used in the password	1
Minimum number of characters to be used in the password	1
Maximum number of consecutive characters in the password	0
Minimum number of special characters required in the password	0

G. Data Archiving Procedures and Guidelines for IRDA Business Analytics Solution

The following table summarizes the marking, transmission, storage, restoration, and destruction procedures / guidelines for information assets classified as **"Restricted", "Confidential"**, and **"Internal".** These procedures / guidelines do not apply to the information assets classified as **"Public".**

Classification	Marking	Transmission	Storage & retention	Destruction
Restricted	**"IRDA Restricted"** prominently printed on a page / displayed on screen, form or presentation media. In case of electronic documents, use footers for marking	**General:** Information is shared with third parties under contractual agreement, appropriate information security controls, audit and appropriate management approval. **Electronic Information:** Authenticate recipient prior to transmission using at least the password (in case of FTP). Ensure complete transmission and receipt by intended party. Use appropriate level of encryption for transmission on public networks and other delivery channels, if required. Password - protect the document and send the document and password separately. **Non-Electronic Information:** Use appropriate	**Electronic Information:** Authenticate individuals requiring access using strong authentication measures. Modification restricted to the information owner or party authorized by information owner. Encryption should be used for privacy protection if necessary. Information is backed up to facilitate recovery of approved backup procedures / guidelines. Backup media should be kept in fire-proof safe. **Non-electronic Information:** Information is not left unattended and	**Electronic Information:** Delete file from storage media using typical system delete commands. If on the hard disk, delete the files before using it for different purpose, or degauss the hard disk removing it from the system. If on CD / Floppy, ensure destruction by shredding it into smaller parts. If on DAT tape, ensure

Classification	Marking	Transmission	Storage & retention	Destruction
		packaging to conceal the contents. Receipt of delivery required. Use registered mail or dedicated carrier. Affix tamper-proof seal on the package. Super-scribe the following on the envelope: **"Private and Confidential"**	should be stored under lock and key. **Retention:** As per contractual / legal requirements. In case of customer data as per regulatory guidelines. As per information owner requirements.	destruction by physical means **Non-Electronic Information:** Destroy using shredder kept in restricted area.
Confidential	**"IRDA Confidential"** prominently printed on a page / displayed on screen, form or presentation media. In case of electronic documents, use footers for marking	**General:** Information is shared with third parties under contractual agreement, appropriate information security controls, audit and appropriate management approval. Sharing of customer information must be in compliance with contract or agreement. **Electronic Information:** Authenticate recipient prior to transmission using at least the password (in case of FTP). Ensure complete transmission and receipt by intended party. Use appropriate level of encryption for transmission on public	**Electronic Information:** Authenticate individuals requiring access using strong authentication measures. Modification restricted to the information owner or party authorized by information owner. Information is backed up to facilitate recovery of approved backup procedures / guidelines.	**Electronic Information:** Delete file from storage media using typical system delete commands. If on hard disk, delete the files before using it for a different purpose or degauss the hard disk If information is highly sensitive, overwrite files. If on CD / Floppy, ensure destruction by

Classification	Marking	Transmission	Storage & retention	Destruction
		networks and other delivery channels, if required. Password - protect the document and send the document and password separately. **Non-Electronic Information:** Use appropriate packaging to conceal the contents. Receipt of delivery required. Use registered mail or dedicated carrier. Affix tamper-proof seal on the package. Super-scribe the following on the envelope: **"Private and Confidential"**	**Non-electronic Information:** Information is not left unattended and should be stored under lock and key. **Retention:** As per contractual / legal requirements. In case of customer data as per regulatory guidelines. As per information owner requirements	shredding it into smaller parts. If on DAT tape, ensure destruction by physical means **Non-Electronic Information:** Destroy using shredder kept in restricted area.
Internal	**"IRDA Internal"** prominently printed on a page / displayed on screen, form or presentation media. In case of electronic documents, use footers for marking	**General:** Information is shared with third parties under contractual agreement. **Electronic Information:** Authenticate recipient prior to transmission using at least the password (in case of FTP). **Non-Electronic Information:** Use appropriate packaging to conceal the contents. Seal on	**Electronic Information:** Modification restricted to the information owner or party authorized by information owner. Information is backed up to facilitate recovery of approved backup procedures / guidelines. Back up media should be kept in a fire proof safe.	**Electronic Information:** Delete file from storage media using typical system delete commands. If on the hard disk, delete the files before using it for different purpose, or degauss the hard disk. If on CD / Floppy,

Classification	Marking	Transmission	Storage & retention	Destruction
		the package.	**Non-electronic Information:** Information is not left unattended and should be stored under lock and key. **Retention:** As per contractual / legal requirements. As per information owner requirements	ensure destruction by shredding it into smaller parts. If on DAT tape, ensure destruction by physical means **Non-Electronic Information:** Destroy using shredder kept in restricted area.

H. Existing applications at IRDA with their details

Functionalities performed by different applications

1. **Content Management System**

Objective:

Frequently used for storing, controlling, versioning, and publishing industry-specific documentation such as news articles, operators' manuals, technical manuals, sales guides, and marketing brochures. The content managed may include computer files, image media, audio files, video files, electronic documents, and Web content. These concepts represent integrated and interdependent layers.

Main Features of CMS:

- Content can be entered manually
- Content of different format such as PDF, Excel, Word are stored
- Content can be downloaded from the portal
- Portal is available in English and Hindi
- Built-in search facility
- Role based content management

Functionality of CMS:

- User Credential verification – This is the security based access method so that the users will proper access rights can access the proper documents and data security is maintained
- Adding of page content – This functionality is used for adding new pages in the portal. Once user log into the system, he can add new contents based on his credentials.
- Modifying a page content – Modifying functionality applies on the existing contents in the portal. If any user wants to modify the content, then he log in the system using his user id and password and depending upon his credentials, he can modify the content.
- Deleting Page Content - This functionality is used for deleting the content already present in the portal. The user logs in the system using his user ID and password. The system verifies his credentials and depending upon his access rights, he can delete the content from the portal. In case the user does not have any deletion rights, system throws a message.
- Search Engine – This functionality is used for searching the contents using some key words.

Once any user input some keyword and hit the search button, then the system starts searching the database and it traces out all those items having matching keyword. In case there is no item matched, then the system shows a message that no item has been found.

2. **Brokers Online Filing System**

Objective:

The main objective of Broker online filing is to provide an online facility for registering new broker, modifying existing brokers' information, filing of returns by brokers.

Functionality of Broker Online Filing:

Registration of brokers with IRDA – The new would-be brokers are required to fill up some forms for registering themselves with IRDA. This facility is available online in this portal. The form required to be filled up for registration is available in this portal. A would-be broker will fill up the form. The data will be automatically stored in database. This data will be visible to IRDA nodal officer who will approve or disapprove the registration on the basis of his offline findings about the data.

Modification and removal of broker's details – This functionality is available for IRDA Nodal officer who can modify or remove the information on brokers whenever necessary. Once the officer receives any communication from the broker regarding modification of details, he can go this portal and change the information as per needed. He can also remove the information about a broker in case he finds anything to do so.

Filing of returns – Brokers files the returns on monthly basis. This functionality of the portal helps them to file the returns online. The returns can be submitted using a pre-defined template. The data submitted will be captured and stored in a database. This data will be used for generating the consolidated reports for audit and internal consumption.

Once the returns are submitted, the broker can also view the summary status report on the following categories;

- Resubmission request
- Returns Filed
- Returns not Filed

The broker can drill down to those reports that are falling in each category.

3. **Grievance Management System**

Objective:

The objective of Grievance management is to monitor the policyholders' grievance and track them for speedy resolution. The grievance management system tracks the new complaint, forwarded complaints, update status of complaints, rending the insurers and generating some customized reports on the basis of the complaints.

Functionality of Grievance Management:

Registering New Complaint – Once IRDA receives any complaint from the policyholders, it registers the complaints after some verification. The newly registered complaint is given a grievance no. and a status. The grievance no. is a unique no and is used to track the complaint for future reference.

Tracking new complaints – IRDA tracks the new complaints along with some basic information on the date of receipt and status of the complaint. The portal is capable of showing the complaints for each insurer and for overall insurers also.

Track the forwarded complaints – This functionality of the portal helps the grievance Department to track the forwarded complaints so that if there is any forwarded complaint which has not been taken care of by the insurer for long, they can send the reminder to the insurers.

Reminder – The system is capable of tracking the complaints which have not been taken care of by the insurers and reminder has been sent to them.

Update Status – The status of the complaints are changed as per the follow up. Such status helps to track the current scenario of the complaints.

Customized Reports – On the basis of the complaints registered, the system is capable of generating some customized reports for each insurer and on an overall basis. Such reports are generated annually and reviewed by IRDA for accessing the complaints status for each insurer and in Indian insurance scenario.

Customized Letters Format – There are three types of letter formats available -

- Acknowledgement letter
- Closed letter
- Update screen for date of filing and insurer reply date

4. **Advertisement Management System**

Objective:

This module is designed to track the details advertisements for each insurer. The module also tracks those advertisements that are released by Intermediaries. The insurers maintain a separate register for tracking the advertisements. So the information captured in the portal helps IRDA to inspect the data maintained by the insurers.

Functionality of Advertisement:

Registering New Advertisement – Once there is some new advertisement for any insurer, then the portal generates the unique insurer-wise advertisement reference no. to track the advertisements and also it sends automatic e-mail to the insurer and the Office-in-Charge (OIC).

Modification of Advertisement – Modification of advertisement is considered as new advertisement and hence the portal generates another advertisement reference no. for the modified advertisements.

Tracking complaints – The insurers has to send the details of the advertisements released to IRDA through hardcopy format. On the receipt of the details, IRDA enters the following details about the advertisement;

- Date of receipt
- IRDA inward No.
- Observations
- Filing of Advertisement details

Notification – The notification is sent to the insurers in the following scenario;

- There is any advertisement which has been launched by the insurer but not provided details .
- If there is any non-compliance in the details of the advertisement, then notification is sent to the insurer.

5. **Third Party Administrators Module**

Objective:

This module is designed to track the details of the third party administrators. Third Party Administrators are engaged by the insurers for fee/ remuneration.

Functionality of Advertisement:

Registration of TPA - The functionality helps the third party administrators to register with IRDA online. Only those licensed Surveyors are eligible for registration with IRDA. The portal contains a form that Surveyors need to fill up for registration. Once the form is submitted, then the data is captured and stored in database. The Officer-in-Charge of IRDA can access the data. He can approve or disapprove on the basis of the data submitted by the Surveyors.

Modification and removal of details of Surveyors – Once a registered Surveyors communicates with the Officer-in-Charge in IRDA about some changes in the details, the officer-in-charge can change the details of the TPA as required and update the data in the system. If there is anything which dictates the removal of TPA, then the OIC also can remove the TPA using the removal functionality.

Querying of data – The portal is capable of querying the data on the basis of the requirements. Once any user runs a particular query, the portal will fetch the relevant data from the database and display the data in a structured predefine format. This feature of the portal helps to generate dynamic reports on the basis of the data on Surveyors.

6. New Business Statistics (Life and Non Life)

Objective:

This module is designed to track the statistics on new business for life & non-life business. The compliance officer of insurer submits the value of the new business statistics for every month to the Officer-in-Charge (OIC) at IRDA.

Functionality of New Business Statistics Module:

Online Submission of Statistics – The insurers submit the new business statistics value on monthly basis to the officer-in-charge in IRDA. Once they submit the values of the new business statistics, the data is stored in the database so that OIC can access the data and validate the same on the basis of the returns submitted by the insurers.

The returns are classified into Individual, group , urban, rural, social sector. Also the portal captures the information on rides.

Security Enabled Accessing Feature – Each insurer is assigned a user ID and a password so that they can submit the new business statistics values and cannot view the details of other insurers. This function helps to maintain data security.

Customized Reporting – Customized reporting capability helps IRDA to consolidate the returns submitted by the insurers and generate reports for each insurer and also for the Indian Insurance industry. The reports are published in the website and IRDA journals after obtaining the approval from

the concerned authority.

Auto-Mailing Feature – This auto-mailing feature sends automated e-mails to the insurers in case there is any delay in submission of the new business statistics values.

Technical Specifications of different existing operational applications

The following data was gathered for different systems based on a questionnaire session organized for capturing the details for various systems

1. **Grievance Management System**

Parameters	Details
System/Application Name	*Grievances Management System(Life & Non-Life)*
System Application Objective and functionality (optional)	Grievances Management for both Life and Non-Life
System Users	Grievances Cell of Life and Non-Life department
System Owner	Grievances Cell of Life and Non-Life department
Data Entry Type	Data entry screen
Frequency of Data Entry	Daily and As & When
Technology used	.NET
Database System	Sql Server 2000 / 2005
Database Size	Less than 1 GB
How many years of data	Since 1 April 2005, 4 Yrs
# of users (IDs created)	10 Users
Hours of peak access	10:00 AM to 2:00 PM and 3PM to 5:30 PM on a week day
Knowledge of structure	IRDA has knowledge about Structure of the tables
How is report generated out of this particular Source System	.Pdf

Parameters	Details
Architecture Type	Web based
Server Hardware Type	HP / IBM X 235
Pain Points and Drawbacks in the system Currently	Some attributes / Classifications not available
Changes and improvement desired in the system	Additional MIS reports required

2. Surveyor Licensing Portal

Parameters	Details
System/Application Name	*Surveyor Licensing System*
System Application Objective and functionality (optional)	Licensing of Surveyors (including trainee surveyors)
System Users	Surveyor Division (Non-Life Department)
System Owner	Surveyor Division (Non-Life Department)
Data Entry Type	Data Entry Screens
Frequency of Data Entry	As and When
Technology used	VB.NET
Database System	Sql Server 2000 / 2005
Database Size	10 Years of Data
How many years of data	5 Years
# of users (IDs created)	5 Users
Hours of peak access	10:00 AM to 2:00 PM and 3PM to 5:30 PM on a week day
Knowledge of structure	IRDA has knowledge about Structure of the tables
How is report generated out of this particular Source System	Crystal report

Parameters	Details
Architecture Type	Client / Server
Server Hardware Type	IBM x 235
Pain Points and Drawbacks in the system Currently	No pain areas
Changes and improvement desired in the system	Web based interface would be required

3. Online Agent Registration

Parameters	Details
System/Application Name	*Agency Licensing Portal*
System Application Objective and functionality (optional)	Issue of Agent Licenses (individual /Corporate/Specified person)
System Users	DPs of Insurers
System Owner	Agent and ATI
Data Entry Type	Data entry screen
Frequency of Data Entry	Daily and As & When
Technology used	ASP / IIS 5.0
Database System	Sql Server 2000
Database Size	5 - 10 GB
How many years of data	9 Yrs
# of users (IDs created)	500 Users
Hours of peak access	10:00 AM to 2:00 PM and 3PM to 5:30 PM on a week day
Knowledge of structure	IRDA has knowledge about Structure of the tables

Parameters	Details
How is report generated out of this particular Source System	Excel
Architecture Type	Web based
Server Hardware Type	HP
Pain Points and Drawbacks in the system Currently	Slow response time, reports take lot of time
Changes desired in the system	Additional functionalities like direct registration of Agents, generation of some additional reports

4. Receipt and Inward System

Parameters	Details
System/Application Name	*Receipt and Inward System*
System Application Objective and functionality (optional)	Tracking of inward mails /office notes
System Users	All staff of IRDA
System Owner	Administration
Data Entry Type	Data entry screen
Frequency of Data Entry	Daily and As & When
Technology used	Developer 2K
Database System	Oracle 9i under Sun Solaris
How many years of data	6 Yrs
# of users (IDs created)	125 Users
Hours of peak access	10:00 AM to 2:00 PM and 3PM to 5:30 PM on a week day

Parameters	Details
Knowledge of structure	IRDA has knowledge about Structure of the tables
How is report generated out of this particular Source System	Reports 2.5 (D2K)
Architecture Type	Client / Server
Server Hardware Type	Sun Fire 250 R
Pain Points and Drawbacks in the system Currently	Slow response time
Changes and improvement desired in the system	Additional functionalities to be included

5. MIS

Parameters	Details
System/Application Name	*MIS*
System Application Objective and functionality (optional)	Collecting Regulatory returns from Insurers and Generating Analysis
System Users	F & A Department
System Owner	F & A Department
Data Entry Type	Data entry screen / Excel template upload
Frequency of Data Entry	Quarterly / Annual
Technology used	VB 6
Database System	Sql Server 2000 / 2005
Database Size	5 Years Data
How many years of data	5 Years
# of users (IDs created)	5 Users (Users of F&A Dept)

Parameters	Details
Hours of peak access	10:00 AM to 2:00 PM and 3PM to 5:30 PM on a week day
Knowledge of structure	IRDA has knowledge about Structure of the tables
How is report generated out of this particular Source System	Crystal Reports / Sql Reporting Services
Architecture Type (if you have a diagram then kindly attach)	Client / Server
Server Hardware Type	IBM x 235
Pain Points and Drawbacks in the system Currently	Reports do not tally with the actual reports submitted by Insurers
Changes and improvement desired in the system	Data filing should be online , Proper validation to be done at Insurer level

6. ATI Database

Parameters	Details
System/Application Name	*ATI Database*
System Application Objective and functionality (optional)	Capturing new application details of ATIs (Online / Off-line)
System Users	Agents and ATI Division
System Owner	Agents and ATI Division
Data Entry Type	Data Entry Screens
Frequency of Data Entry	As and When
Technology used	Developer 2K
Database System	Oracle 9i under Sun Solaris

Parameters	Details
Database Size	3-4 Years Data
How many years of data	3 Years
# of users (IDs created)	5 Users
Hours of peak access	10:00 AM to 2:00 PM and 3PM to 5:30 PM on a week day
Knowledge of structure	IRDA has knowledge about Structure of the tables
How is report generated out of this particular Source System	Reports 2.5 (D2K)
Architecture Type	Client / Server
Server Hardware Type	Sun Fire 250 R