**Conceptual Solution Architecture**

**For**

**IAM Tactical Master Data Management**

|  |  |
| --- | --- |
| Project Name | Tactical MDM |
| INVP # (if known) |  |
| ITLT Sponsor | Simon Jenner |
| Enterprise Architect | Stuart Ledingham |
| Principle Architect | Naresh Deenadayalan |
| Solution Architect | Raghav Mirthipati |
| Data Architect | Harsh Mundel |
| Infrastructure Architect | Raghav Venkat Mirthipati |
| Security Architecture | Marcos Larkman |
| BP&I Security Integration Lead | Basav Mahadevaiah |

**Document Control**

Classification INTERNAL USE / CONFIDENTIAL

Owner *Naresh Deenadayalan*

Author *Naresh Deenadayalan*

Creation Date: 09/12/2020

Version 0.6

Status Review

Location Architecture Group Site

Template version v2.12

**Contents:**

1 Business Vision 4

2 Business Scenarios 4

2.1 MDM Use Cases 4

3 Stakeholders and their Concerns 5

4 Constraints 5

4.1 Timeline Constraints 5

4.2 Business Organization Constraints 5

4.3 IT Organization Constraints 5

4.4 External and Regulatory Constraints 5

4.5 Budgetary Constraints 5

5 Business Architecture 6

5.1 Business Domains 6

5.2 Security Architecture 6

6 MDM Framework and Model 6

6.1 SQL Server Integration Services (SSIS) 7

6.2 Data Quality Services (DQS) 7

6.3 Master Data Services (MDS) 7

7 Users and User Experience Expectations 8

8 Current State 8

8.1 Current Workforce data sources 8

8.2 Interim Workforce Data Sources 9

9 Assumptions 9

10 High Level Solution Architecture 10

10.1 Proposed Interim Architecture (Tactical MDM Solution) 10

10.2 IAM Original State Architecture 10

11 Technology Disposition Implications 11

12 Integration Architecture 12

12.1 MDM Integration with SuccessFactors 12

12.2 MDM Integration with ACG database 13

12.3 MDM Integration with US SAP ECC 13

12.4 MDM Integration with SAIL point 14

13 Information Architecture 14

13.1 Data storage 14

13.2 Data flow model 15

13.2.1 Data flow from Source system to SSIS 15

13.2.2 Dataflow within SSIS packages 16

13.2.3 Dataflow from MDS to Sailpoint 16

13.3 Golden Record 17

13.3.1 Business Rules set 17

13.4 Logical Attributes SuccessFactors 17

13.5 Logical Attributes US SAP ECC 19

13.6 Logical Attributes ACG 22

14 End User Compute Architecture 23

15 Infrastructure / Hosting Architecture 23

15.1 NG US Azure Data centre topology 24

15.2 Deployment Consideration 24

16 Infrastructure / Network Architecture 25

16.1 NG US High Level Design 25

17 Performance Requirements 25

18 Backup Requirements 25

19 Disaster Recovery Requirements 26

19.1 SQL Always on cluster for SQL DB 26

20 Key Non-Functional Requirements 27

21 Security Architecture 27

21.1 Information Classification / Criticality 27

21.2 Regulatory Impacts 28

21.3 Baseline Security Requirements (BSR’s) 29

21.4 Security Tower Engagement 29

# Business Vision

Self-assessment by IT management, along with work by our internal and external audit teams, has highlighted substantial opportunities for improvement. Underlying these observations is the lack of an end to end user lifecycle processes leading to incomplete, or inaccurate, user master data. This situation is further compounded by a fragmented underlying system architecture requiring substantial manual processing and leading to a lack of real-time transparency on user access status.

This project is looking to implement a tactical solution which introduces the concepts of Master Data Management and creates a new Global Worker ID which will carry over into a strategic solution which is unique to an individual regardless of employment type or status.

# Business Scenarios

Currently workers of different types are mastered in multiple source systems with no global unique worker identifier. Each source system has its own internal identifiers with overlaps in some data across repositories.

There is no single holistic view of workforce data (all people working in National Grid including employees, contingent and MSP) – the worker identity master data is spread across multiple repositories

Some MSPs are in SuccessFactors (for learning purposes) and remain in ECC (US) and ACG -DB (UK) where they are mastered

IAM processes requires a unique worker id to be provided to SailPoint.

## MDM Use Cases

|  |  |
| --- | --- |
| Use Case | Benefit |
| Centralized data repository for worker identity master data from multiple WDD systems of record | All worker identity master data in one place, one governance and control process |
| Create unique enterprise persistent worker identity | Single unique identifier that carries throughout the life cycle of the worker at NG and required by IAM and more |
| Allow data quality improvement, remove data duplication, and allow data steward to see data issues and help making decision | Consistency maintain data quality of the worker identity master data |
| Create and maintain golden master record of workforce data and sync cleanse and standardise data back to WDD systems of record | Removed data discrepancy between different source systems |
| National Grid to have an authoritative and reliable source of workforce master data | This solve the one biggest pain points of IAM |
| Master workforce data source for EDP | Consistent clean accurate worker identity master data for the EDP |

# Stakeholders and their Concerns

* Human Resources
* IT Management

# Constraints

## Timeline Constraints

1. Required ports and connections to be made available soon between the source systems and the MDM across UK and US Azure data centres to allow the deployment activities begin
2. Ability to achieve the new tactical MDM solution for the Global workforce by April 2021

## Business Organization Constraints

1. Rapid project deployment of the ADAM partners
2. Data integrity checks and MSP process improvement items will still need completing for either option​

## IT Organization Constraints

1. Production version of ACG-DB (source system for UK-MSP) is not available yet in NG landscape
2. Access to complete and accurate National Grid application/systems inventory information
3. Worker identity master data accuracy and completeness
4. Availability of obfuscated test data for end to end testing due to GDPR controls

## External and Regulatory Constraints

1. Changes/projects currently running on the source system (SF, US SAP ECC, ACG DB)

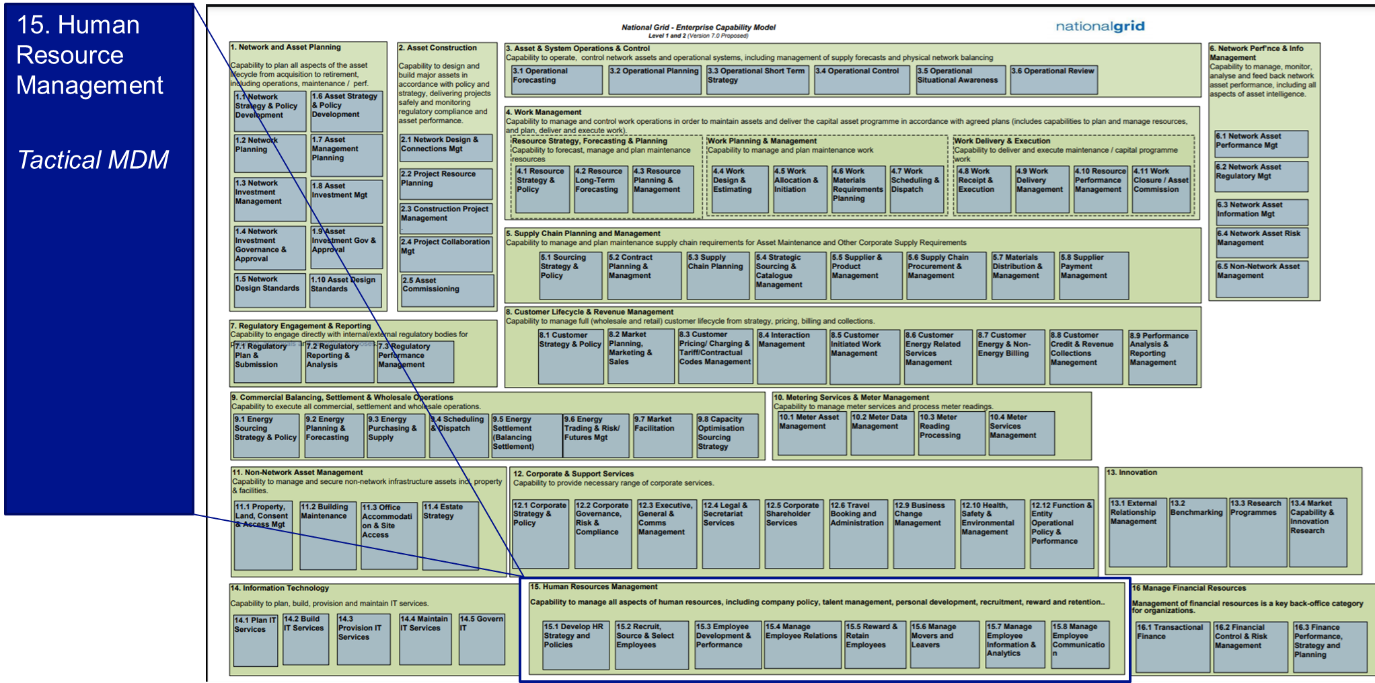
## Budgetary Constraints

1. Onboarding ADAM partners
2. Technical debt

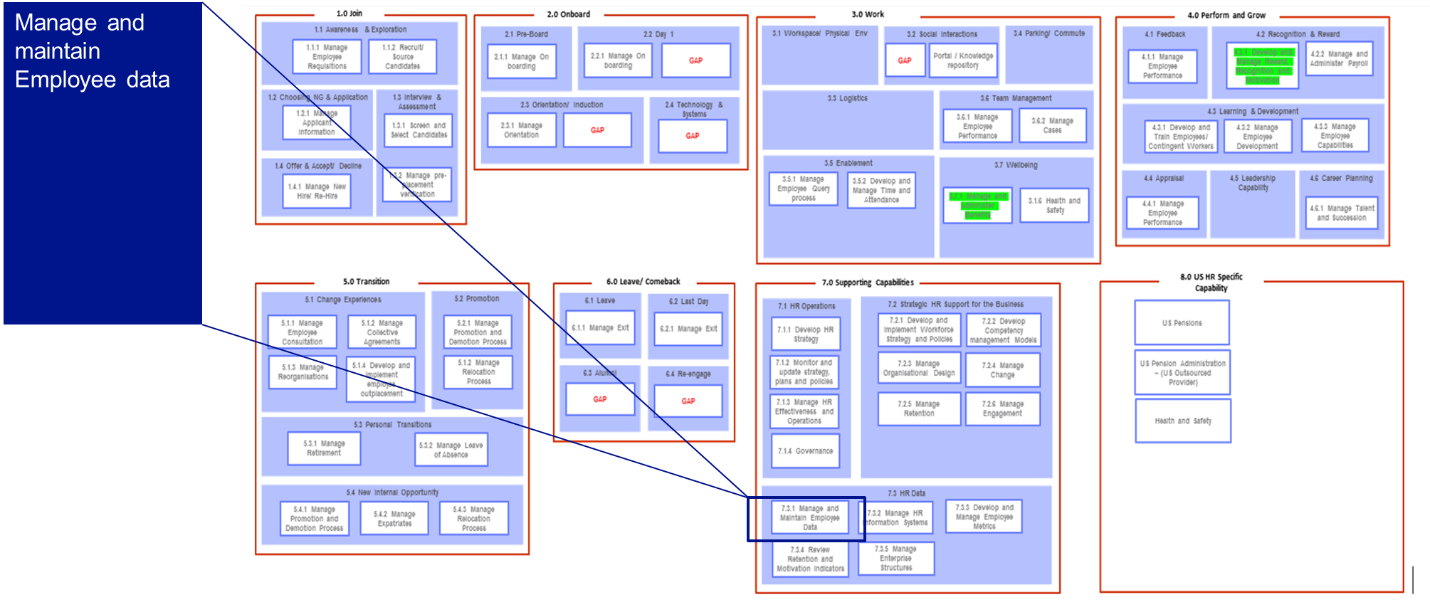
# Business Architecture

## Business Domains

The following Enterprise Capability Model shows has been assessed, and the key impacted area as part of the IAM-MDM tactical solution is Human Resource Management, which is highlighted below



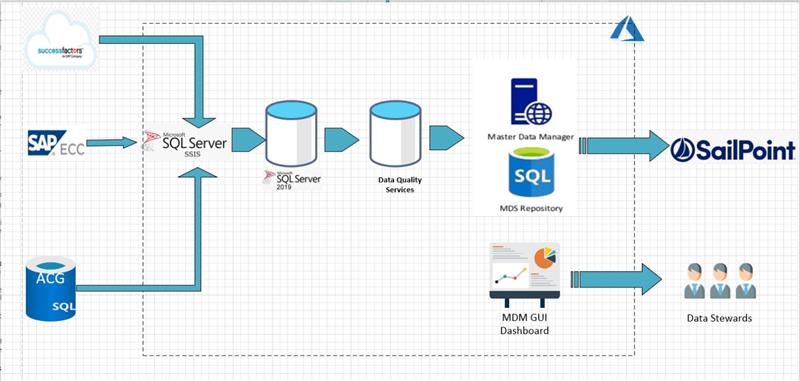
## HR Capability model



# MDM Framework and Model

Master data management (MDM), defines a process of collecting enterprise data from various sources, applying standard rules and business processes, building a single view of the data, and finally distributing the ‘golden’ version of data to various systems in the enterprise, thereby making it accessible to the consumers

Microsoft has implemented the MDM concepts with SQL server approach using Master Data Services (MDS), Data Quality Services (DQS) and Integration Services (SSIS).



## SQL Server Integration Services (SSIS)

SQL Server Integration Services is a platform for building enterprise-level data integration and data transformations solutions. Integration Services can extract and transform data from a wide variety of sources such as XML data files, flat files, and relational data sources, and then load the data into one or more destinations.

In the context of MDM tactical solution, SSIS will read the .CSV files produced by the source systems SuccessFactors, SAP ECC, ACG Database and process them into the data quality services

## Data Quality Services (DQS)

SQL Server Data Quality Services (DQS) is a knowledge-driven data quality product. DQS enables you to build a knowledge base and use it to perform a variety of critical data quality tasks, including correction, enrichment, standardization, and de-duplication of your data. DQS enables you to perform data cleansing by using cloud-based reference data services provided by reference data providers. DQS also provides you with profiling that is integrated into its data-quality tasks, enabling you to analyze the integrity of your data.

DQS performs the data integrity checks on the records retrieved from the source systems before loading the data into Master data Services repository

## Master Data Services (MDS)

Master Data Services enables you to manage a master set of your organization's data. You can organize the data into models, create rules for updating the data, and control who updates the data.

The records retrieved from the DQS will be loaded into the respective tables in MDS repository, which will be consumed by IAM(SailPoint)

A User Interface would be provided to the Data Stewards to access the MDS records inorder resolve any conflicts identified in the records

# Users and User Experience Expectations

Following are the user personas identified as part of the scope of this solution and their impact accordingly

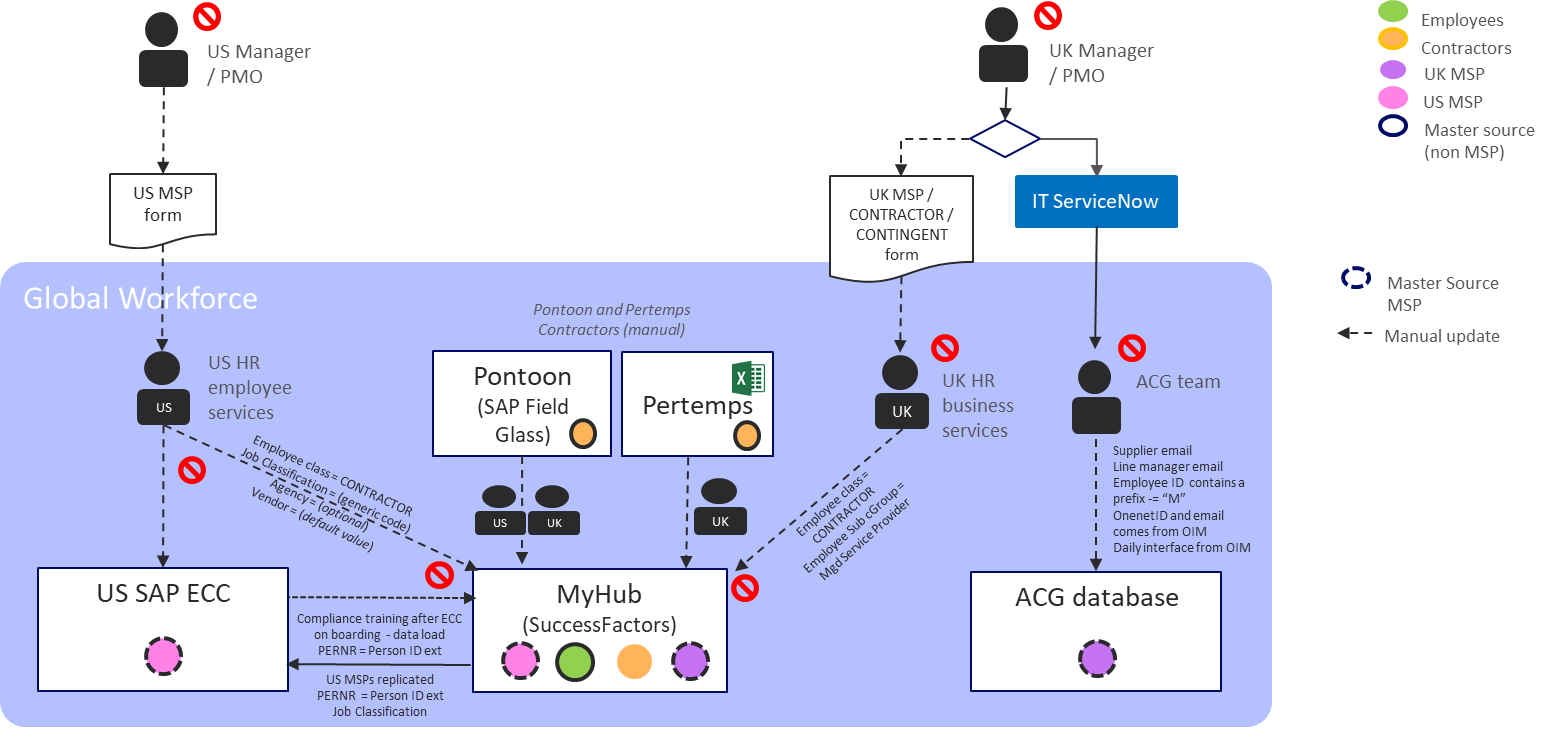
**In Scope User Personas**

|  |  |  |
| --- | --- | --- |
| Persona | Interacting Internal/External  to Corp Network | User Impact or User Expectations |
| Data Stewards | Internal to Corp Network | Data stewards would be provided with a GUI to the MDM tool to resolve any conflicts in the worker identity master data, and for analytical reporting purpose |

# Current State

## Current Workforce data sources

Currently the workers of different types are mastered in multiple source systems with no global unique worker identifier. Each source system has its own internal identifiers with overlaps in some data across repositories.

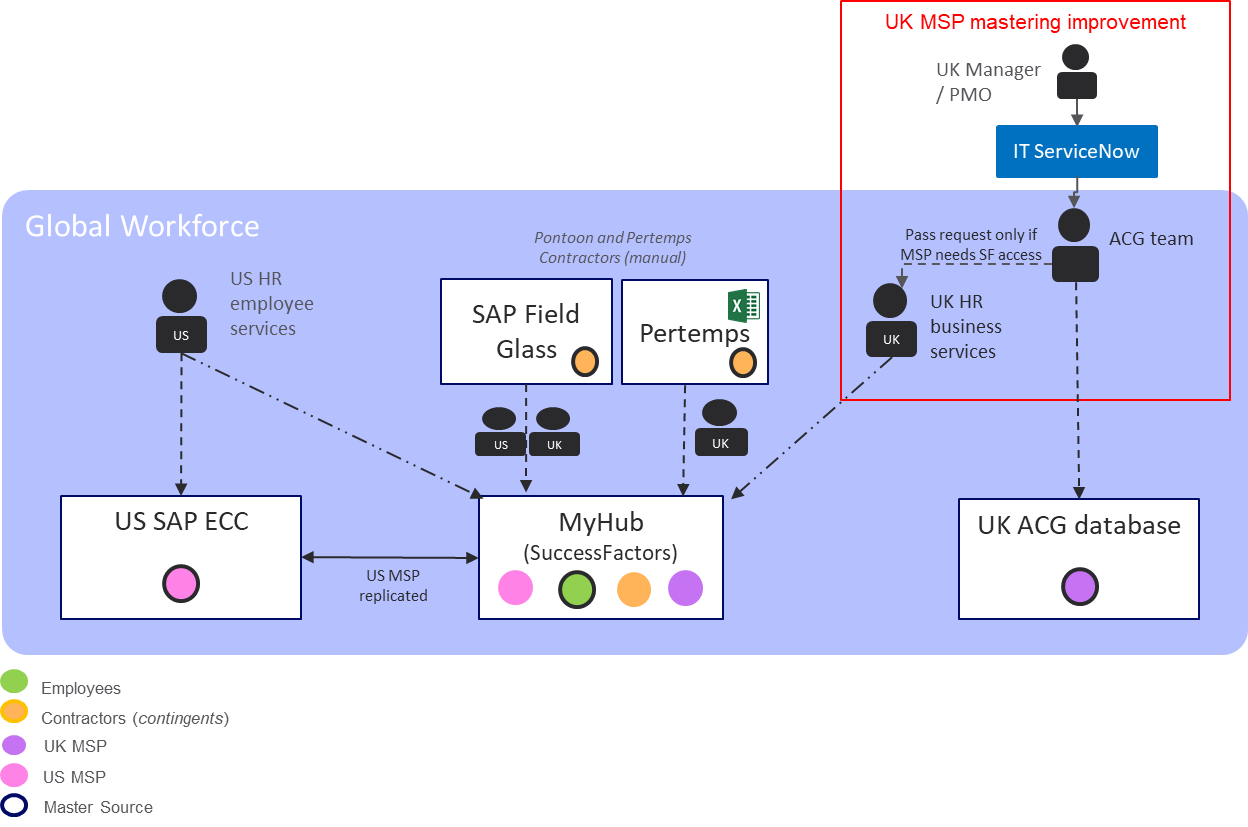


|  |  |
| --- | --- |
| Workforce Type | Master System |
| Employees | SuccessFactors |
| Contractors | SAP Fieldglass & Pertemps |
| MSPs | US SAP ECC/ACG Database/Success factors |

1. US MSPs
   1. Duplicate requests for the same person (leading to duplicate records)
   2. Leavers process – end dates not being provided at source (lack of control) or may be entered incorrectly
   3. Manual data inconsistencies occur from time to time
2. UK MSPs
   1. Multiple entry point for UK MSP with potential for duplication due to manual process.
   2. UK ACG should be source of truth but there are duplications (approx. 500+)

## Interim Workforce Data Sources

In the interim state, it is proposed that UK MSPs are mastered in the ACG Database to support the MDM tactical solution



# Assumptions

|  |  |
| --- | --- |
| # | Assumption |
| 1 | SuccessFactors will be the central authoritative source of employees and contractors and US SAP ECC for Managed Service Providers (US). UK MSPs will be in ACG database. |
| 2 | This is a Tactical Solution only for IAM consumption |
| 3 | Required business rules sets to identify the unique record would be defined by the business during the requirement phase |
| 4 | Data from MDM will not be updated back to the source system as part of this tactical solution |
| 5 | The required environments for Source systems, MDM and IAM would be made available on time |
| 6 | DR will be managed using Azure site recovery |

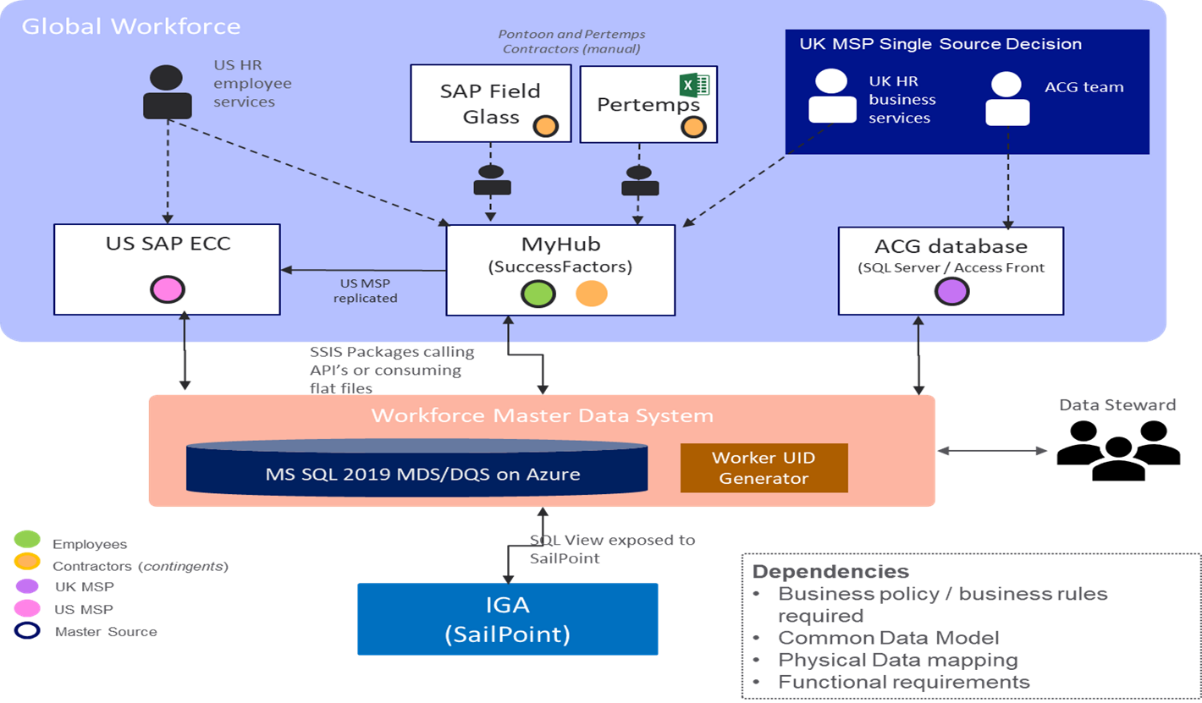
# High Level Solution Architecture

## Proposed Interim Architecture (Tactical MDM Solution)

The following diagram shows the proposed interim architecture of the Tactical MDM solution

The worker identity master data from the SuccessFactors, ACG Database and US SAP ECC system will be fed into the MDM tool. Based on the business rule sets defined in the MDM,

the unique worker ID (Golden record) will be generated which will then be sent across to IAM (SailPoint)



## IAM Original State Architecture

Please refer to the appendix for the Original Proposed IAM architecture.

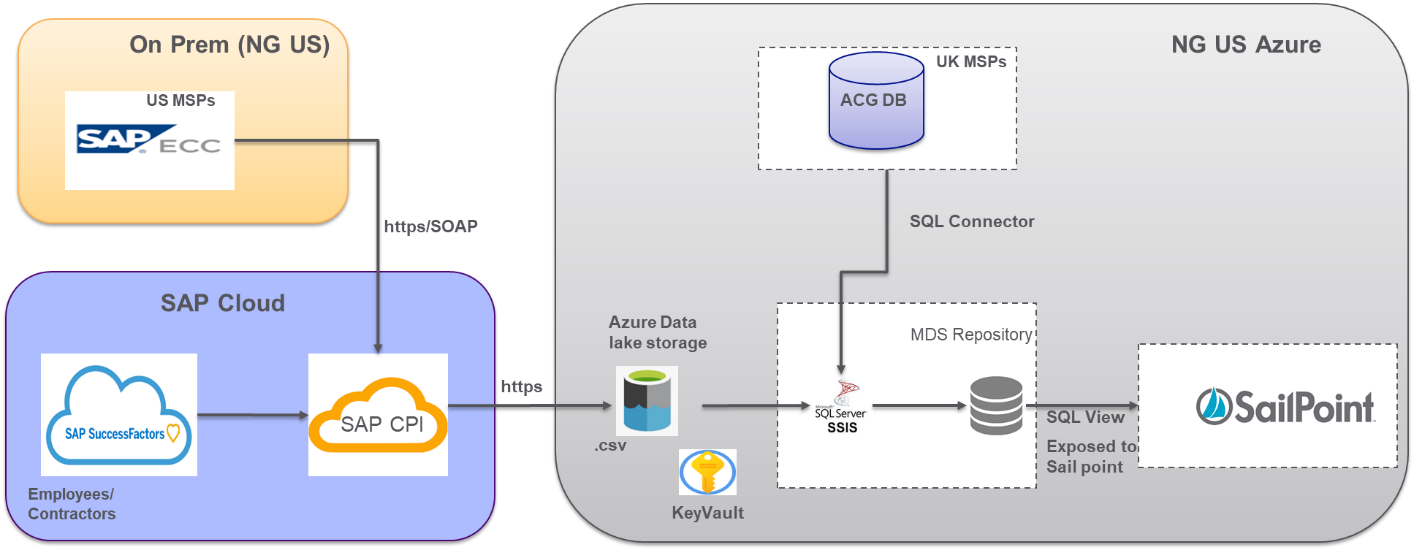
# Technology Disposition Implications

|  |  |
| --- | --- |
| List All Proposed *New* Technology | Capabilities |
| 1. Master data Services | Master Data services is a Microsoft tool for supporting Master Data Management (MDM), providing capability to have a centralised database for the Workforce data and enables data provision to IAM (Sailpoint) |

|  |  |
| --- | --- |
| List All Proposed *Replaced or Retired* Technology | Capabilities |
| N/A | N/A |

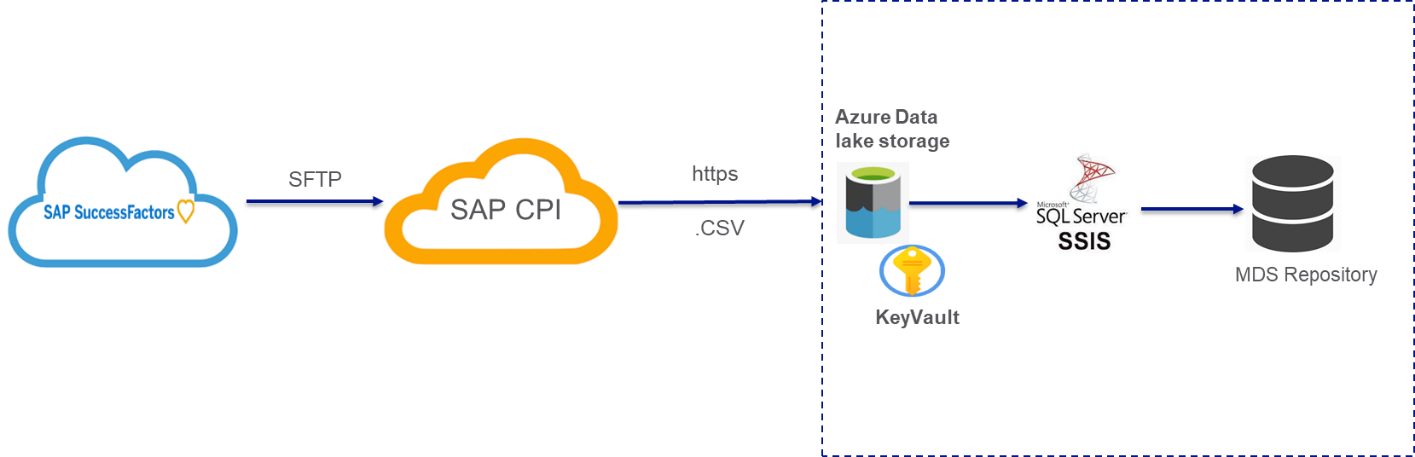
# Integration Architecture

The following diagram shows the High-level integration pattern for the connection between the source systems and the MDM tool



|  |  |  |
| --- | --- | --- |
| System | Data Context | Integration Pattern |
| SuccessFactors | US and UK Permanent Employee  and contingent workers | SAP CPI middleware transferring data from SuccessFactors to MDM SQL Database over https |
| US SAP ECC | US MSPs | SAP CPI transferring data from ECC to MDM SQL database over https |
| ACG Database | UK MSPs | Standard SSIS to SQL connectors |
| IAM (SailPoint) | Golden Records | Standard SailPoint connectors to consume the SQL view exposed by MDM |

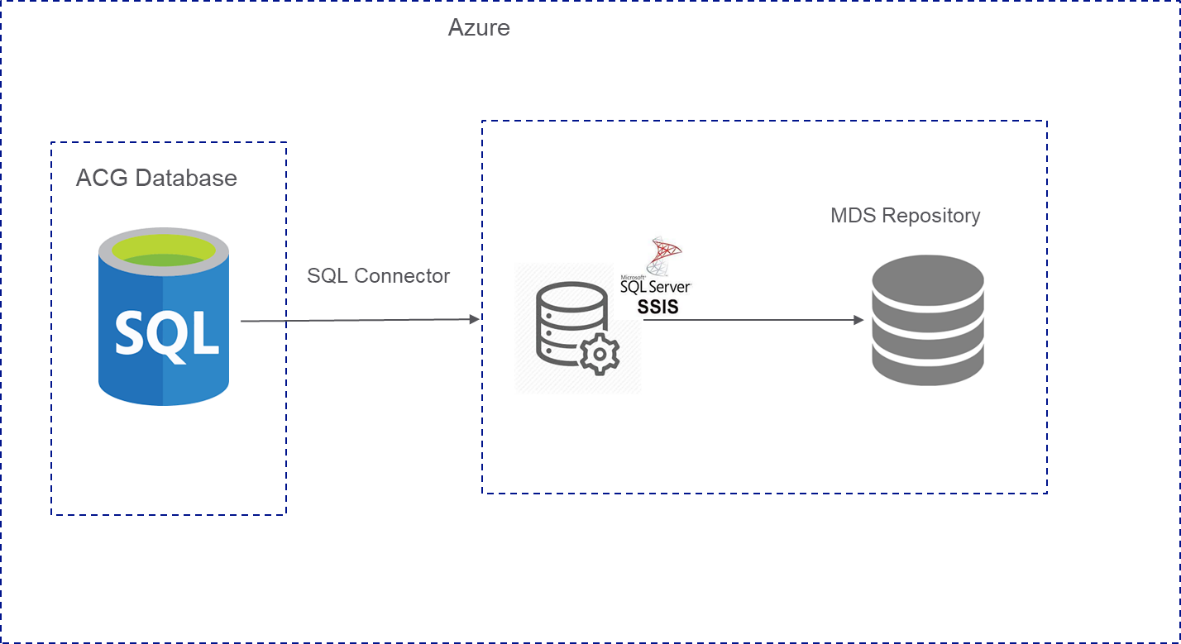
## MDM Integration with SuccessFactors



* Employees and Contractors data will be sent from SuccessFactors system to the MDM via the SAP CPI
* Data from SuccessFactors will be pulled by the CPI Interface and converted into an encrypted .CSV file
* The encrypted file will be placed at staging location in NG US Azure, wherein SSIS package will pick up the file and process into MDS repository
* Only the incremental records will be pulled from the SuccessFactors
* The records would be pulled for every 4 hours

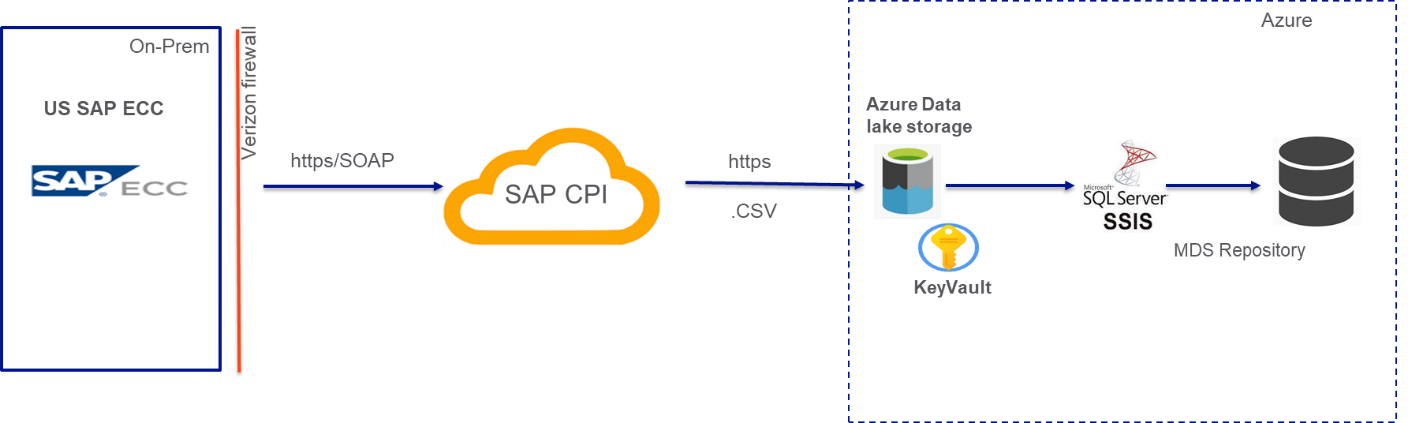
## MDM Integration with ACG database

Standard SQL connector would be utilized to integrate the SSIS and the ACG SQL database



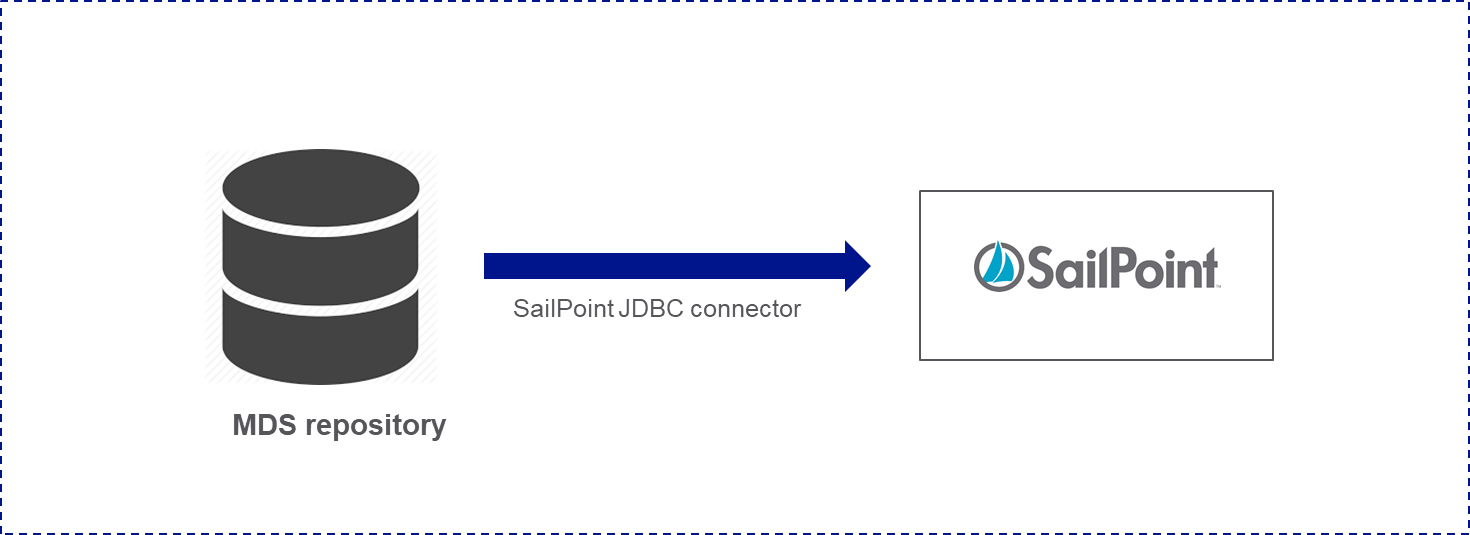
## MDM Integration with US SAP ECC

US SAP ECC will be integrated with MDM via the SAP CPI middleware layer



* US MSPs records from SAP ECC will be pushed to CPI interface as an idoc process
* The will be converted into an encrypted .CSV file
* The encrypted file will be placed at staging location in NG US Azure, wherein SSIS package will pick it up and process into MDS repository
* Only the incremental records will be pulled from the SuccessFactors
* The records would be pulled for every 4 hours

## MDM Integration with SAIL point



* Out of box SailPoint JDBC connector will be used to connect to the MDS SQL server
* The MDS data would be exposed as SQL view for the SailPoint to consume

# Information Architecture

## Data storage

The workforce data for MDM will be obtained from the following 3 source systems

* + - 1. Success factors – Employee & contingent/contractors
      2. US SAP ECC – US MSP
      3. ACG-DB – UK MSP

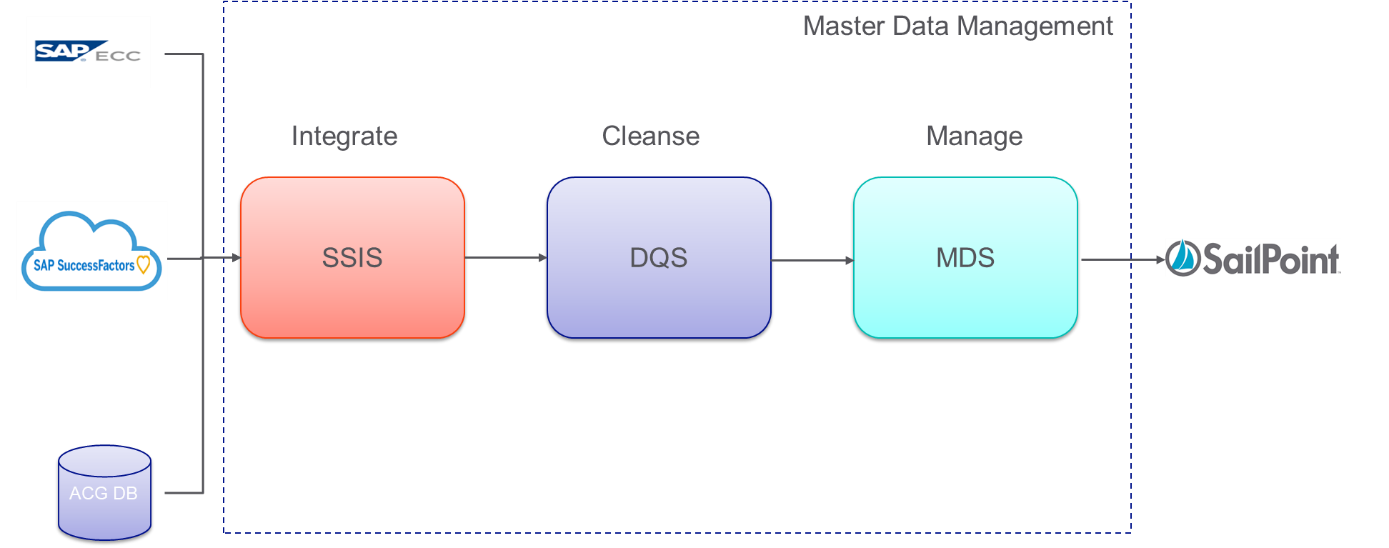
The data will be stored in Master Data Services repository in SQL server and required business rules will be applied to the records using the fuzzy logic to identify the Golden record with unique worker id which will then be sent to the IAM (SailPoint) systems

## Data flow model

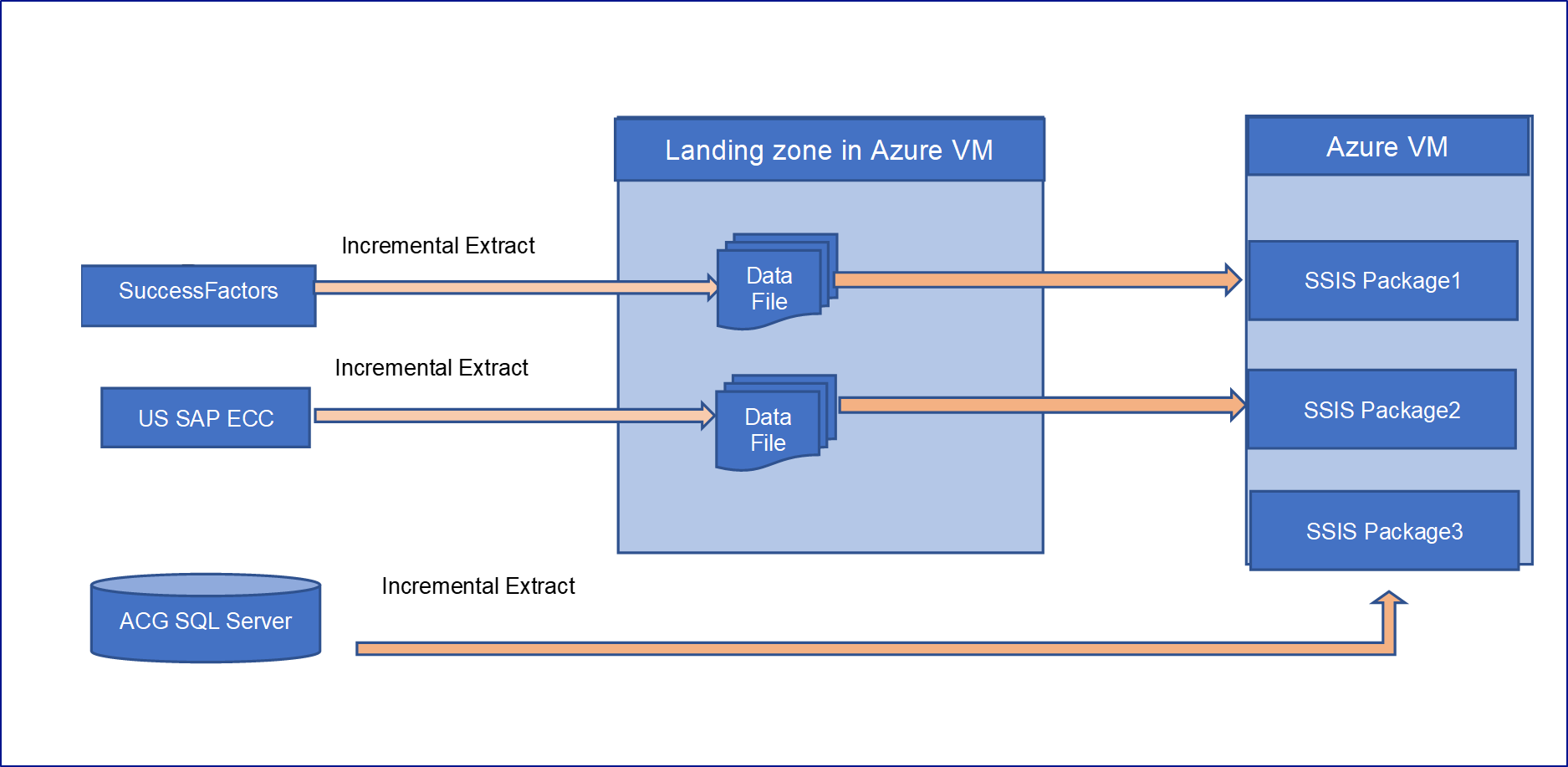
The following diagram shows the end to end data flow model from the source systems to the IAM (sail point) via MDM

* Data from the master sources (SuccessFactors, US SAP ECC, ACG DB) will be transferred to a staging location in Azure VM via a secure channel in .CSV file format
* The source files will be picked by the SSIS Package and will be transferred to Data quality services (DQS) to perform data integrity checks
* Post the validation, the record will be loaded into the MDS database layer
* The Database table will be exposed as a SQL view for the SailPoint to consume using standard SailPoint JDBC connector

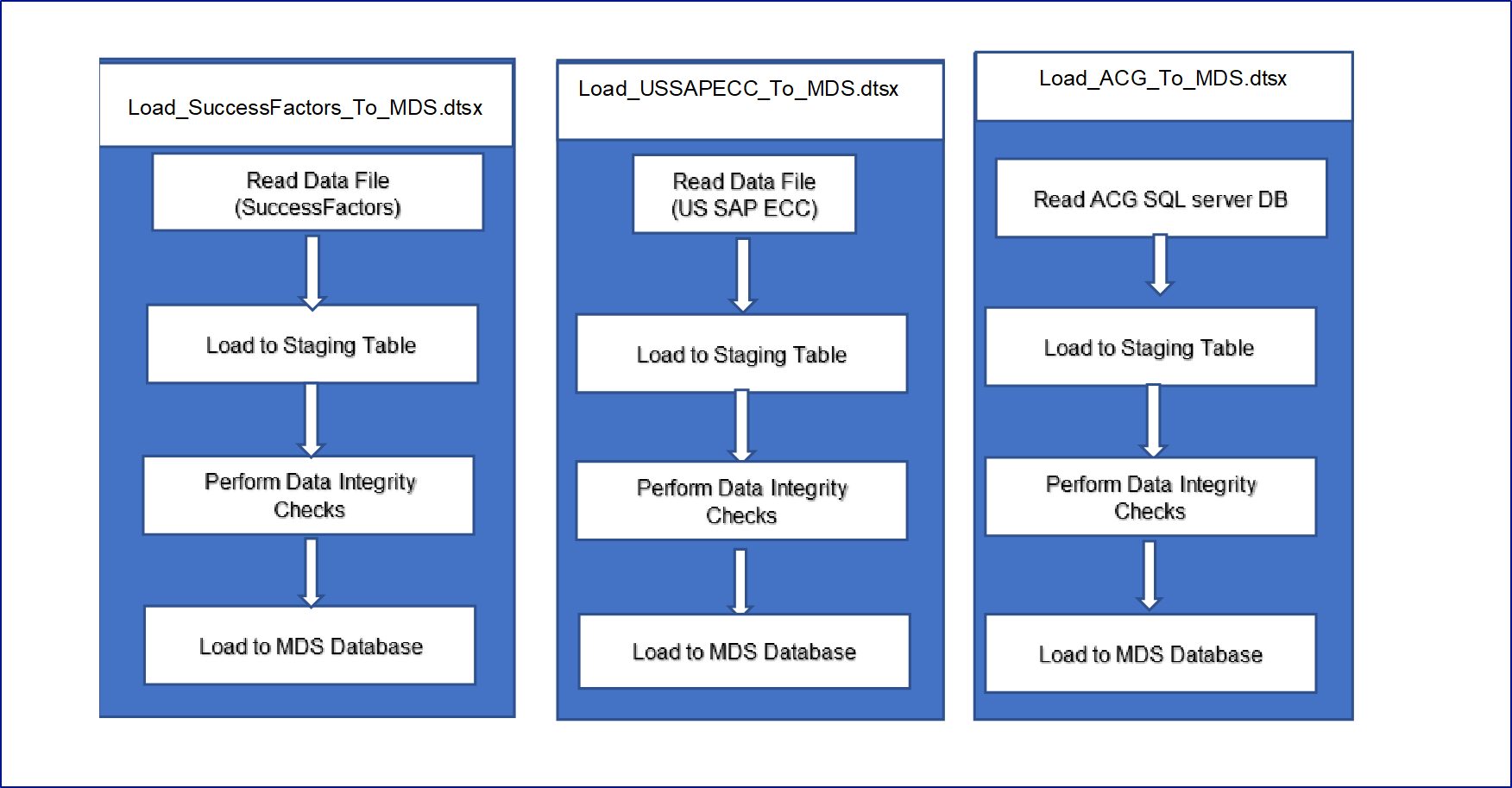
Three SSIS packages will be created to read the worker data from SuccessFactors, SAP ECC and ACG respectively. SSIS Package is a .dtsx file



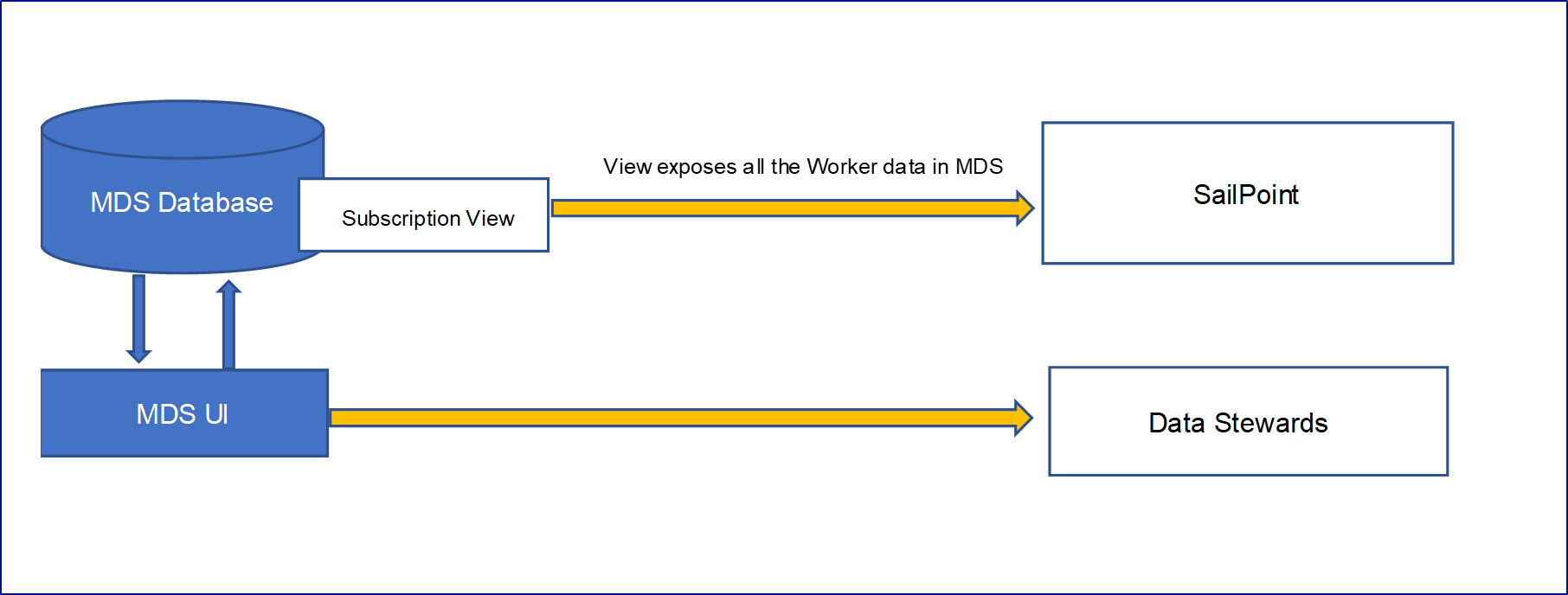
### Data flow from Source system to SSIS



### Dataflow within SSIS packages



### Dataflow from MDS to Sailpoint



## Golden Record

A workforce Golden Record is an accurate, complete and comprehensive representation of the attributes need to uniquely identify a worker

It will

* Have a comprehensive, unambiguous, and up-to-date view of a WORKER
* Enhanced security & reduced exposure to risk due to access issues
* Ensure better data integration & en-route to greater degree of self service and automation
* Enable reliable reporting & data visualisation

Once the MDM receives the worker record from the respective source system, following set of business rules will be applied to generate a unique ID agnostic of the source systems called the Golden record

### Business Rules set

Following are the business rules set executed in MDM to generate the Golden record

|  |  |
| --- | --- |
| SI.NO | Business Rules Priority |
| 1 | Match the records in below order. If the record matches the first Source ID, then don’t move to next Source ID. |
| 1.) If (SAP PERNR) in ECC US = MDM (SAP PERNR) |
| 2.) If (PERSON ID EXTERNAL) in SuccessFactors = MDM (PERSON ID EXTERNAL) |
| 3.) If ACG ID (UNIQUE ID) = MDM (UNIQUE ID) |
| 2 | Match NG Email Address with MDM NG Email Address. |
| Match the domain name of the email address |
| 3 | Fuzzy Match First Name, Last Name |
| 4 | Match NG Manager Email Id |
| 5 | Match Preferred First Name and Preferred Last name |

Please refer to the attached document for the list of matching attributes



## Logical Attributes SuccessFactors

Employees and Contractors data are held in the SuccessFactors system, following are the attributes which would be transferred to the MDM tool in

*\*This list will be further revised post a dry run in MDS, and the attributes which are required for arriving at the Golden record will only be needed*

|  |  |  |
| --- | --- | --- |
| IAM Target Attribute Name | Source Attribute Name | Mandatory(Yes/No) |
| First Name | EmployeeCentral.personalInfo.first-name | Yes |
| Last Name | EmployeeCentral.personalInfo.last-name | Yes |
| Preferred First Name | EmployeeCentral.personalInfo.formal-name | Yes |
| Preferred Last Name | EmployeeProfile.personalinfo.custom-string1 | Yes |
| Worker Unique ID |  | No |
| User ID (SF) | EmployeeProfile.Standard.userId | Yes |
| Source System Worker ID | EmployeeCentral.personInfo.person-id-external | Yes |
| Business Unit |  | No |
| Business Unit Code |  | No |
| Division | For Employee -EmployeeCentral.JobInfo.Position.Division  For Contingent/MSP - EmployeeCentral.Joblnfo.division | Yes |
| Division Code | For Employee -EmployeeCentral.JobInfo.Division | Yes |
| Department |  | No |
| Department Code |  | No |
| Location | EmployeeCentral.Joblnfo.location | Yes |
| Address | EmployeeProfile.Standard.addressLine1 | Yes |
| City | EmployeeProfile.Standard.city | Yes |
| State/County | EmployeeProfile.Standard.state | Yes |
| Country | EmployeeCentral.JobInfo.Country-Of-Company | Yes |
| Company | EmployeeCentral.JobInfo.company | Yes |
| Job Title | For Employee -EmployeeCentral.JobInfo.Position.jobTitle  For Contingent/MSP - EmployeeCentral.JobInfo.job-title or EmployeeCentral.JobInfo.Position.jobTitle | Yes |
| Job Code | EmployeeCentral.JobInfo.job-code | Yes |
| Position Code | EmployeeCentral.JobInfo.position | Yes |
| Position Title | For Employee - EmployeeCentral.JobInfo.Position.jobTitle  For Contingent/MSP - EmployeeCentral.JobInfo.job-title | Yes |
| Employee Type | EmployeeCentral.JobInfo.EmployeeType [custom-string1] - As its custom field, will be removed as part of MyHR2.0 - If values are "employee or non-employee" then its not employee class | Yes |
| Employee Class | EmployeeCentral.JobInfo.Employee-Class | Yes |
| Employee SubGroup\* | For Employee -EmployeeCentral.JobInfo.Employment-Type | Yes |
| Vendor Name\* | For Employee - N/A  For Contingent/MSP - EmployeeCentral.WorkOrder.vendor [using this navigate to Vendor object and read VendorInfo.vendorName | Yes |
| Vendor ID\* | For Employee - N/A  For Contingent/MSP - EmployeeCentral.WorkOrder.vendor [using this navigate to Vendor object and read VendorInfo.vendorCode | Yes |
| Employee Status | EmployeeCentral.JobInfo.EmployeeStatus | Yes |
| Cost Centre ID | EmployeeCentral.JobInfo.cost-center | Yes |
| Cost Centre | EmployeeCentral.JobInfo.cost-center | Yes |
| Manager ID | EmployeeCentral.JobInfo.manager-id | Yes |
| Start Date | EmployeeCentral.employmentInfo.start-date | Yes |
| Termination Date | EmployeeCentral.employmentInfo.end-date | Yes |
| Employee Band | EmployeeCentral.employmentInfo.custom-string33 | Yes |
| US\_BD\_PRA001 Learning Course Complete Date | DevLearning\_4202.PA\_LRN\_ITEM\_CMPL\_EVENT.COMPLETION\_DATE  - You have to do lookup of this date using the course name, userID - DevLearning\_4202 is the LMS system 's technical name | No |
| US\_TLD\_NERC010 Learning Course Complete Date | For Contingent/MSP - DevLearning\_4202.PA\_LRN\_ITEM\_CMPL\_EVENT.COMPLETION\_DATE  - You have to do lookup of this date using the course name, userID - DevLearning\_4202 is the LMS system 's technical name | No |
| US\_BD\_NERC001 Learning Course Complete Date | DevLearning\_4202.PA\_LRN\_ITEM\_CMPL\_EVENT.COMPLETION\_DATE  - You have to do lookup of this date using the course name, userID - DevLearning\_4202 is the LMS system 's technical name | No |
| US\_BD\_NERC002 Learning Course Complete Date | DevLearning\_4202.PA\_LRN\_ITEM\_CMPL\_EVENT.COMPLETION\_DATE  - You have to do lookup of this date using the course name, userID - DevLearning\_4202 is the LMS system 's technical name | No |
| Event Name | For Employee - EmployeeCentral.JobInfo.Event For Contingent/MSP - EmployeeCentral.JobInfo.Event-Reason | Yes |
| Event Reason Name | EmployeeCentral.JobInfo.Event-Reason | Yes |
| Email Address | EmployeeCentral.EmailInfo.Email-Address [where IsPrimary = Yes] | Yes |
| OneNet ID | EmployeeCentral.userAccountInfo.user-name | Yes |
| Legal Entity | EmployeeCentral.JobInfo.Company | Yes |
| Division L1 Name | EmployeeCentral.JobInfo.Division - use this to navigate to "Division" object and get cust\_DivisionL1 | Yes |
| Division L2 Name | EmployeeCentral.JobInfo.Division - use this to navigate to "Division" object and get cust\_DivisionL2 | Yes |
| Division L3 Name | EmployeeCentral.JobInfo.Division - use this to navigate to "Division" object and get cust\_DivisionL3 | Yes |
| Division L4 Name | EmployeeCentral.JobInfo.Division - use this to navigate to "Division" object and get cust\_DivisionL4 | Yes |
| Division L5 Name | EmployeeCentral.JobInfo.Division - use this to navigate to "Division" object and get cust\_DivisionL5 | Yes |
| Division L6 Name | EmployeeCentral.JobInfo.Division - use this to navigate to "Division" object and get cust\_DivisionL6 | Yes |
| First Name | Infotype – Personal Data: First Name PA0002.VORNA |  |
| Last Name | Infotype – Personal Data: Last Name PA0002.NACHN |  |
| Preferred First Name | N/A |  |
| Preferred Last Name | N/A |  |
| Worker Unique ID |  |  |
| User ID (SF) | Infotype 0105 – Communication subtype 0001: System ID PA0105.USRID where PA0105.SUBTY = '0001' |  |
| Source System Worker ID | PA0000.PERNR |  |
| Business Unit | N/A |  |
| Business Unit Code |  |  |
| Division | Z Object relationship to O Object (Organizational unit) Not visible on Person’s record  GM: I think this is N/A as there is no true division reference on SAP |  |
| Division Code | N/A |  |
| Department | O Object (Organizational unit) Visible on person’s IT01 Organizational Plan section PA0001.ORGEH then lookup HRP1000.STEXT Where HRP100.OBJID = PA0001.ORGEH |  |
| Department Code | O Object (Organizational unit) Visible on person’s IT01 Organizational Plan section PA0001.ORGEH |  |
| Location | T500P Visible on all person’s infotypes as Header GM: do you want location code and location name or just location name? T500P.NAME1 where T500P.PERSA = PA0001.VDSK1 |  |
| Address | T500P Visible on all person’s infotypes as Header GM: What is the plan if a location has two address lines. T500P.STRAS where T500P.PERSA = PA0001.VDSK1 |  |
| City | T500P Not visible on person’s record T500P.ORT01 where T500P.PERSA = PA0001.VDSK1 |  |
| State/County | T500P Not visible on person’s record T500P.REGIO where T500P.PERSA = PA0001.VDSK1 |  |
| Country | T500P Not visible on person’s record |  |
| Company | PA0001.BURKS GM: do you want company code and company name? |  |
| Job Title | C Object (Job) Visible on person’s IT01 Organizational Plan section HRP1000.STEXT where HRP1000.OTYPE = 'C' and HRP1000.OBJID = PA0001.STELL |  |
| Job Code | C Object (Job) Visible on person’s IT01 Organizational Plan section PA0001.STELL |  |
| Position Code | S Object (Position) Visible on person’s IT01 Organizational Plan section PA0001.PLANS |  |
| Position Title | S Object (Position) Visible on person’s IT01 Organizational Plan section HRP1000.STEXT where HRP1000.OTYPE = 'S' and HRP1000.OBJID = PA0001.PLANS |  |
| Employee Type | N/A - although possibly derived from employee group and subgroup |  |
| Employee Class | Employee Group and Employee Subgroup Visible on all person’s infotypes as Header PA0001.PERSG |  |
| Employee SubGroup\* | PA0001.PERSK |  |
| Vendor Name\* |  |  |
| Vendor ID\* |  |  |
| Employee Status | Infotype Actions (Employment) Visible on all person’s infotypes as Header PA0000.STAT2 |  |
| Cost Centre ID | K Object (Cost Center) relationship to O Object (Organizational unit) Visible on person’s IT01 Enterprise structure section PA0001.KOSTL |  |
| Cost Centre | K Object (Cost Center) relationship to O Object (Organizational unit) Visible on person’s IT01 Enterprise structure section HRP1000.STEXT where HRP1000.OTYPE = 'K' and HRP1000.OBJID = PA0001.KOSTL |  |
| Manager ID | Based on A/012 relationship between S Object (Position) and O Object (Organizational Unit. Not visible on person’s record |  |
| Start Date | Infotype 00 Start Date Visible on all person's infotypes as Header GM: are you really looking for start date here or hire date or rehire date? |  |
| Termination Date | Infotype 00 End Date Visible on all person’s infotypes as Header PA0041. PA0041.DATXX where PA0041.DARXX = '04' |  |
| Employee Band | PA0008.TRFGR |  |
| US\_BD\_PRA001 Learning Course Complete Date | N/A |  |
| US\_TLD\_NERC010 Learning Course Complete Date | Same as above as some contractors do need NERC/CIP |  |
| US\_BD\_NERC001 Learning Course Complete Date | Same as above as some contractors do need NERC/CIP |  |
| US\_BD\_NERC002 Learning Course Complete Date | Same as above as some contractors do need NERC/CIP |  |
| Event Name | T529A.MNTXT Where T529A.MASSN = PA0000.MASSN |  |
| Event Reason Name | T530.MGTXT Where T530.MASSN = PA000.MASSN and T530.MASSG = PA0000.MASSG |  |
| Email Address | PA0105.USRID\_LONG where PA0105.SUBTY = '0010' |  |
| OneNet ID | PA0105.USRID Where PA0105.SUBTY = '0001' |  |
| Legal Entity | PA0001.BURKS GM: do you want company code and company name? |  |
| Division L1 Name | N/A or use default values from other interfaces |  |
| Division L2 Name | N/A or use default values from other interfaces |  |
| Division L3 Name | HRP1000.STEXT where HRP1000.OTYPE = 'ZA' - get PA0001.ORGEH then find HRP10001 ZA relationship on HRP1001 between ZA Object and O Object where HRP1001.OTYPE = 'O' and HRP1001.OBJID = PA0001.ORGEH and HRP1001.SCLAS = 'ZA'  This is US logic only |  |
| Division L4 Name | HRP1000.STEXT where HRP1000.OTYPE = 'ZB' - get PA0001.ORGEH then find HRP10001 ZB relationship on HRP1001 between ZB Object and O Object where HRP1001.OTYPE = 'O' and HRP1001.OBJID = PA0001.ORGEH and HRP1001.SCLAS = 'ZB'  This is US logic only |  |
| Division L5 Name | HRP1000.STEXT where HRP1000.OTYPE = 'ZC' - get PA0001.ORGEH then find HRP10001 ZC relationship on HRP1001 between ZC Object and O Object where HRP1001.OTYPE = 'O' and HRP1001.OBJID = PA0001.ORGEH and HRP1001.SCLAS = 'ZC''  This is US logic only |  |
| Division L6 Name | HRP1000.STEXT where HRP1000.OTYPE = 'ZD' - get PA0001.ORGEH then find HRP10001 ZD relationship on HRP1001 between ZD Object and O Object where HRP1001.OTYPE = 'O' and HRP1001.OBJID = PA0001.ORGEH and HRP1001.SCLAS = 'ZD'  This is US logic only |  |
| First Name | msp\_First\_Name | Yes |
| Last Name | msp\_Last\_Name | Yes |
| Preferred First Name | N/A |  |
| Preferred Last Name | N/A |  |
| Worker Unique ID | msp\_Unique\_ID\_pk | Yes |
| User ID (SF) | msp\_OneNet\_ID | No |
| Source System Worker ID | ACGMDB.\_MspMgmt.t\_MSP\_Details.msp\_Unique\_ID\_pk | Yes |
| Business Unit | msp\_Business\_Entity | Yes |
| Business Unit Code | N/A |  |
| Division | msp\_Function | Yes |
| Division Code | N/A |  |
| Department | msp\_Department | Yes |
| Department Code | N/A |  |
| Location | msp\_Primary\_Location | Yes |
| Address | N/A |  |
| City | N/A |  |
| State/County | N/A |  |
| Country | msp\_Region | Yes |
| Company | msp\_Supplier | Yes |
| Job Title | N/A |  |
| Job Code | N/A |  |
| Position Code | N/A |  |
| Position Title | N/A |  |
| Employee Type | N/A |  |
| Employee Class | N/A |  |
| Employee SubGroup\* | N/A |  |
| Vendor Name\* | N/A |  |
| Vendor ID\* | N/A |  |
| Employee Status | N/A (can be derived from the End Date) |  |
| Cost Centre ID | N/A (can be derived from the NG Line Manager Details by lookup to Success Factors data) | No |
| Cost Centre | N/A (can be derived from the NG Line Manager Details by lookup to Success Factors data) | No |
| Manager ID | msp\_NG\_LM\_EmpID | Yes |
| Start Date | msp\_Start\_Date | Yes |
| Termination Date | msp\_End\_Date | Yes |
| Employee Band | N/A |  |
| US\_BD\_PRA001 Learning Course Complete Date | N/A |  |
| US\_TLD\_NERC010 Learning Course Complete Date | N/A |  |
| US\_BD\_NERC001 Learning Course Complete Date | N/A |  |
| US\_BD\_NERC002 Learning Course Complete Date | N/A |  |
| Event Name | N/A |  |
| Event Reason Name | N/A |  |
| Email Address | msp\_Worker\_NG\_email | No |
| OneNet ID | msp\_OneNet\_ID | No |
| Legal Entity | msp\_Business\_Entity | Yes |
| Division L1 Name |  | No |
| Division L2 Name |  | No |
| Division L3 Name |  | No |
| Division L4 Name |  | No |
| Division L5 Name |  | No |
| Division L6 Name |  | No |

## Logical Attributes US SAP ECC

US SAP ECC would be the master source system for the US MSP worker data and following are the logical attributes that would flow from US SAP ECC to MDM

|  |  |  |
| --- | --- | --- |
| IAM Target Attribute Name | Source Attribute Name | Mandatory(Yes/No) |
| First Name | Infotype – Personal Data: First Name PA0002.VORNA |  |
| Last Name | Infotype – Personal Data: Last Name PA0002.NACHN |  |
| Preferred First Name | N/A |  |
| Preferred Last Name | N/A |  |
| Worker Unique ID |  |  |
| User ID (SF) | Infotype 0105 – Communication subtype 0001: System ID PA0105.USRID where PA0105.SUBTY = '0001' |  |
| Source System Worker ID | PA0000.PERNR |  |
| Business Unit | N/A |  |
| Business Unit Code |  |  |
| Division | Z Object relationship to O Object (Organizational unit) Not visible on Person’s record  GM: I think this is N/A as there is no true division reference on SAP |  |
| Division Code | N/A |  |
| Department | O Object (Organizational unit) Visible on person’s IT01 Organizational Plan section PA0001.ORGEH then lookup HRP1000.STEXT Where HRP100.OBJID = PA0001.ORGEH |  |
| Department Code | O Object (Organizational unit) Visible on person’s IT01 Organizational Plan section PA0001.ORGEH |  |
| Location | T500P Visible on all person’s infotypes as Header GM: do you want location code and location name or just location name? T500P.NAME1 where T500P.PERSA = PA0001.VDSK1 |  |
| Address | T500P Visible on all person’s infotypes as Header GM: What is the plan if a location has two address lines. T500P.STRAS where T500P.PERSA = PA0001.VDSK1 |  |
| City | T500P Not visible on person’s record T500P.ORT01 where T500P.PERSA = PA0001.VDSK1 |  |
| State/County | T500P Not visible on person’s record T500P.REGIO where T500P.PERSA = PA0001.VDSK1 |  |
| Country | T500P Not visible on person’s record |  |
| Company | PA0001.BURKS GM: do you want company code and company name? |  |
| Job Title | C Object (Job) Visible on person’s IT01 Organizational Plan section HRP1000.STEXT where HRP1000.OTYPE = 'C' and HRP1000.OBJID = PA0001.STELL |  |
| Job Code | C Object (Job) Visible on person’s IT01 Organizational Plan section PA0001.STELL |  |
| Position Code | S Object (Position) Visible on person’s IT01 Organizational Plan section PA0001.PLANS |  |
| Position Title | S Object (Position) Visible on person’s IT01 Organizational Plan section HRP1000.STEXT where HRP1000.OTYPE = 'S' and HRP1000.OBJID = PA0001.PLANS |  |
| Employee Type | N/A - although possibly derived from employee group and subgroup |  |
| Employee Class | Employee Group and Employee Subgroup Visible on all person’s infotypes as Header PA0001.PERSG |  |
| Employee SubGroup\* | PA0001.PERSK |  |
| Vendor Name\* |  |  |
| Vendor ID\* |  |  |
| Employee Status | Infotype Actions (Employment) Visible on all person’s infotypes as Header PA0000.STAT2 |  |
| Cost Centre ID | K Object (Cost Center) relationship to O Object (Organizational unit) Visible on person’s IT01 Enterprise structure section PA0001.KOSTL |  |
| Cost Centre | K Object (Cost Center) relationship to O Object (Organizational unit) Visible on person’s IT01 Enterprise structure section HRP1000.STEXT where HRP1000.OTYPE = 'K' and HRP1000.OBJID = PA0001.KOSTL |  |
| Manager ID | Based on A/012 relationship between S Object (Position) and O Object (Organizational Unit. Not visible on person’s record |  |
| Start Date | Infotype 00 Start Date Visible on all person's infotypes as Header GM: are you really looking for start date here or hire date or rehire date? |  |
| Termination Date | Infotype 00 End Date Visible on all person’s infotypes as Header PA0041. PA0041.DATXX where PA0041.DARXX = '04' |  |
| Employee Band | PA0008.TRFGR |  |
| US\_BD\_PRA001 Learning Course Complete Date | N/A |  |
| US\_TLD\_NERC010 Learning Course Complete Date | Same as above as some contractors do need NERC/CIP |  |
| US\_BD\_NERC001 Learning Course Complete Date | Same as above as some contractors do need NERC/CIP |  |
| US\_BD\_NERC002 Learning Course Complete Date | Same as above as some contractors do need NERC/CIP |  |
| Event Name | T529A.MNTXT Where T529A.MASSN = PA0000.MASSN |  |
| Event Reason Name | T530.MGTXT Where T530.MASSN = PA000.MASSN and T530.MASSG = PA0000.MASSG |  |
| Email Address | PA0105.USRID\_LONG where PA0105.SUBTY = '0010' |  |
| OneNet ID | PA0105.USRID Where PA0105.SUBTY = '0001' |  |
| Legal Entity | PA0001.BURKS GM: do you want company code and company name? |  |
| Division L1 Name | N/A or use default values from other interfaces |  |
| Division L2 Name | N/A or use default values from other interfaces |  |
| Division L3 Name | HRP1000.STEXT where HRP1000.OTYPE = 'ZA' - get PA0001.ORGEH then find HRP10001 ZA relationship on HRP1001 between ZA Object and O Object where HRP1001.OTYPE = 'O' and HRP1001.OBJID = PA0001.ORGEH and HRP1001.SCLAS = 'ZA'  This is US logic only |  |
| Division L4 Name | HRP1000.STEXT where HRP1000.OTYPE = 'ZB' - get PA0001.ORGEH then find HRP10001 ZB relationship on HRP1001 between ZB Object and O Object where HRP1001.OTYPE = 'O' and HRP1001.OBJID = PA0001.ORGEH and HRP1001.SCLAS = 'ZB'  This is US logic only |  |
| Division L5 Name | HRP1000.STEXT where HRP1000.OTYPE = 'ZC' - get PA0001.ORGEH then find HRP10001 ZC relationship on HRP1001 between ZC Object and O Object where HRP1001.OTYPE = 'O' and HRP1001.OBJID = PA0001.ORGEH and HRP1001.SCLAS = 'ZC''  This is US logic only |  |
| Division L6 Name | HRP1000.STEXT where HRP1000.OTYPE = 'ZD' - get PA0001.ORGEH then find HRP10001 ZD relationship on HRP1001 between ZD Object and O Object where HRP1001.OTYPE = 'O' and HRP1001.OBJID = PA0001.ORGEH and HRP1001.SCLAS = 'ZD'  This is US logic only |  |

## Logical Attributes ACG

ACG would be the master source system for the UK MSP worker data and following are the logical attributes that would flow from ACG to MDM

|  |  |  |
| --- | --- | --- |
| IAM Target Attribute Name | Source Attribute Name | Mandatory(Yes/No) |
| First Name | msp\_First\_Name | Yes |
| Last Name | msp\_Last\_Name | Yes |
| Preferred First Name | N/A |  |
| Preferred Last Name | N/A |  |
| Worker Unique ID | msp\_Unique\_ID\_pk | Yes |
| User ID (SF) | msp\_OneNet\_ID | No |
| Source System Worker ID | ACGMDB.\_MspMgmt.t\_MSP\_Details.msp\_Unique\_ID\_pk | Yes |
| Business Unit | msp\_Business\_Entity | Yes |
| Business Unit Code | N/A |  |
| Division | msp\_Function | Yes |
| Division Code | N/A |  |
| Department | msp\_Department | Yes |
| Department Code | N/A |  |
| Location | msp\_Primary\_Location | Yes |
| Address | N/A |  |
| City | N/A |  |
| State/County | N/A |  |
| Country | msp\_Region | Yes |
| Company | msp\_Supplier | Yes |
| Job Title | N/A |  |
| Job Code | N/A |  |
| Position Code | N/A |  |
| Position Title | N/A |  |
| Employee Type | N/A |  |
| Employee Class | N/A |  |
| Employee SubGroup\* | N/A |  |
| Vendor Name\* | N/A |  |
| Vendor ID\* | N/A |  |
| Employee Status | N/A (can be derived from the End Date) |  |
| Cost Centre ID | N/A (can be derived from the NG Line Manager Details by lookup to Success Factors data) | No |
| Cost Centre | N/A (can be derived from the NG Line Manager Details by lookup to Success Factors data) | No |
| Manager ID | msp\_NG\_LM\_EmpID | Yes |
| Start Date | msp\_Start\_Date | Yes |
| Termination Date | msp\_End\_Date | Yes |
| Employee Band | N/A |  |
| US\_BD\_PRA001 Learning Course Complete Date | N/A |  |
| US\_TLD\_NERC010 Learning Course Complete Date | N/A |  |
| US\_BD\_NERC001 Learning Course Complete Date | N/A |  |
| US\_BD\_NERC002 Learning Course Complete Date | N/A |  |
| Event Name | N/A |  |
| Event Reason Name | N/A |  |
| Email Address | msp\_Worker\_NG\_email | No |
| OneNet ID | msp\_OneNet\_ID | No |
| Legal Entity | msp\_Business\_Entity | Yes |
| Division L1 Name |  | No |
| Division L2 Name |  | No |
| Division L3 Name |  | No |
| Division L4 Name |  | No |
| Division L5 Name |  | No |
| Division L6 Name |  | No |

# End User Compute Architecture

Standard National Grid laptops will be used.

# Support

|  |  |
| --- | --- |
| Support Type | Description |
| First Line | First Line Support will exist in alignment with existing National Grid methods and will require interaction with the IT Helpdesk and or SNOW in order to initiate a call which will be assessed by the Helpdesk and routed accordingly if an immediate resolution is not available |
| Second Line Azure | Azure (IAAS) support will be provided by IBM team, please refer to the link [here](https://nationalgridplc.sharepoint.com/:w:/r/sites/GRP-INT-US-CloudandHostingDeliveryCenter/_layouts/15/Doc.aspx?sourcedoc=%7B40AA3669-DEA7-45CE-A114-9C136635A38F%7D&file=IBM%20support(%20L%20EN%20ENT).docx&action=default&mobileredirect=true) for IBM service catalogue |
| Second Line Application (MDM) | *<To be confirmed>* |
| Second Line SAP Interfaces | Wipro Application Support team supports the SAP Interfaces from Source system |

Further details on support model would be updated in Service Operating Model (SOM) which is considered as one of the output of this Project.

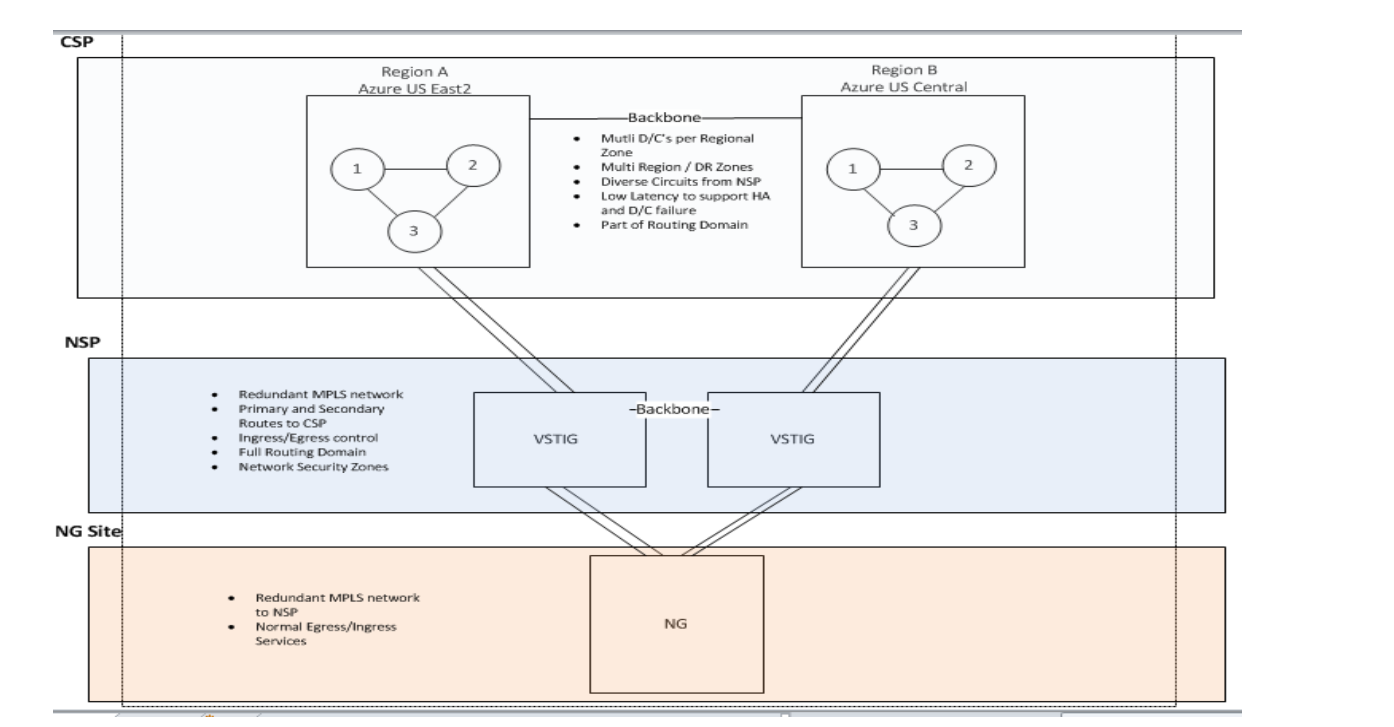
# Infrastructure / Hosting Architecture

The MDM tactical solution will be hosted in the NG US Azure data centre



|  |  |
| --- | --- |
| Location | Description |
| East US 2 | Will act as the **primary** **site** as bulk of the user population resides in US. |
| Central US | Will act as the **secondary/disaster recovery** site to offer redundancy. |

## NG US Azure Data centre topology



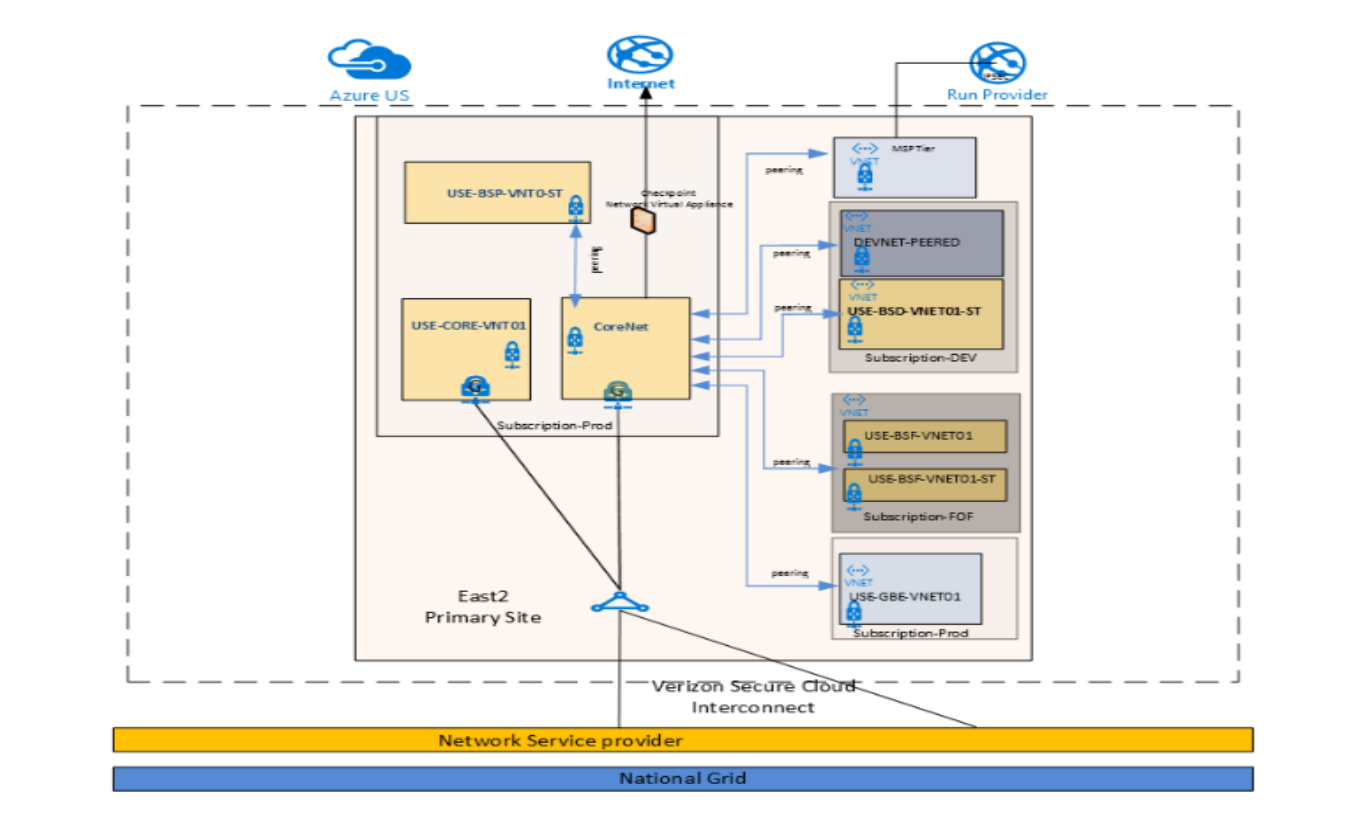
## Deployment Consideration

|  |  |
| --- | --- |
| Component | Description |
| MDS | Master data services |
| SSIS | SSIS packages load the data into MDS staging tables |

# Infrastructure / Network Architecture

|  |  |
| --- | --- |
| VNET | Subnet |
| CoreNet VNET | PROD-DB |
| DEVNET-PEERED | Business service Development  (App/DB subnet) |
| USE-BSF-VNT01  VNET | Business service FOF/QA  (App/Db subnet) |

## NG US High Level Design



# Performance Requirements

No critical requirements identified at this stage

# Backup Requirements

As the solution is deployed in Azure standard Azure backup services will be used.

* Backup – daily, 7day retention
* Disk and database backup

Standard Azure Backups:

* VM/OS Backups is scheduled via Azure Recovery Vault.
* Database Backups are done thru native tools

1. SQLServer – SQL dumps to blob storage account using power shell at database host level. SQL dumps are storage in hot storage accounts for 60 days after which they get moved to cold storage account.

* VM snapshots are done using Azure backup on-demand basis (maintenance/patching etc.)

1. Standard Retention- Data Lifecycle Management

The table below shows the Standard VM backup policy:

|  |  |
| --- | --- |
| Backup Frequency | Retention Period |
| Retention of Daily Backup | Daily at 11:30 pm for 7 days |
| Retention of Weekly Backup | Sunday at 11:30 pm for 4 Weeks |
| Retention of Monthly Backup | First Sunday at 11:30 pm for 12 Months |
| Retention of Yearly Backup | First Sunday in January at 11:30pm for 3Years |

* Database Backups (Dumps):
* transactional every 4 hours – retained for 7 days
* daily differential – retained for 7 days
* weekly (Sundays) full dumps – retained for 4 weeks
* monthly full dumps (1st of every month) - retained for 12 months
* year-end full dumps (1st day of Jan) – retained for 3 years
* Azure Restore Time for Azure backups (VM/DB)

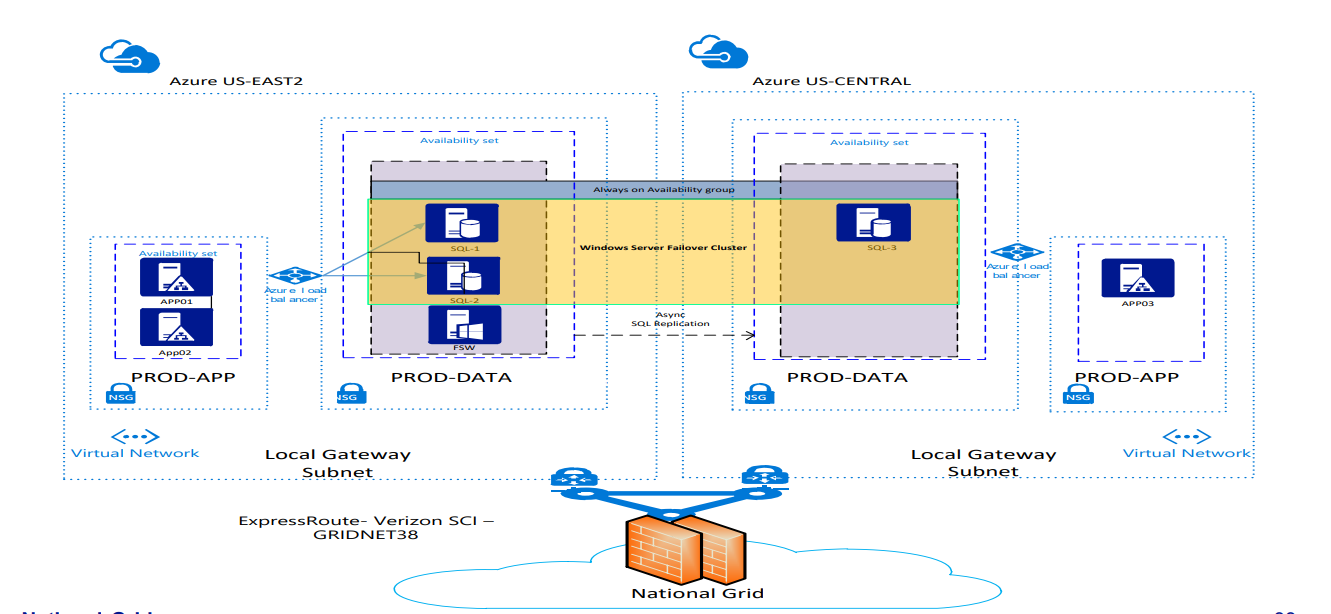
Following is typical restore time:

* 250 GB VM – < 4 hours once the ticket is submitted.
* 250 GB SQL DB – < 4 hours once the ticket is submitted.
* >250 GB VM or SQL DB - include additional 15 minutes for every additional 100GB of data.

# Disaster Recovery Requirements

* Disaster Recovery using ASR and SQL always on.
* Active-passive mode leveraging Azure regional pairs US East 2 and US Central
* High Availability provided via Azure availability sets
* RTO – <= 30 minutes
* RPO – <=15 mins

## SQL Always on cluster for SQL DB



# Key Non-Functional Requirements

|  |  |  |  |
| --- | --- | --- | --- |
| Req. No. | Category | Requirement | MOSCOW |
| 1 | Availability/ Maintenance | At least 99.9 % availability for all the components across the entire solution | S |
| 2 | Disaster Recovery | Recovery Point Objectives (RPO) <= 15 min across all the components for the entire solution | S |
| 3 | Disaster Recovery | Recovery Time Objectives (RTO) <= 30 mins across all the components for the entire solution | S |
| 4 | Regulatory Requirement | Leavers should be disabled within 24 hours | S |
| 5 | Data Files Availability | Data Files from SAP Systems should be available every 4 hours | S |
| 6 | Data Files Availability | IAM (SailPoint) will fetch the records from MDM for every 6 hours | S |

# Security Architecture

## Information Classification / Criticality

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Public | Internal Use | Confidential | Strictly Confidential |
| Operationally Critical | Forbidden | Private | Private | Private |
| Critical | Private / Hybrid | Private / Hybrid | Private / Hybrid | Private |
| Core | Public / Private / Hybrid | Public / Private / Hybrid | Public / Private / Hybrid | Public / Private / Hybrid |
| Efficiency & Performance | Public / Private / Hybrid | Public / Private / Hybrid | Public / Private / Hybrid | Public / Private / Hybrid |

## Regulatory Impacts

|  |  |  |
| --- | --- | --- |
| Regulatory regime | Description | In Scope (yes / no) |
| NERC CIP (US) | North American Electric Reliability Corporation critical infrastructure protection | No |
| CRITICAL ELECTRIC (ENERGY) INFRASTRUCTURE INFORMATION (CEII) | US regulation covering specific engineering, vulnerability, or detailed design information about proposed or existing critical infrastructure | No |
| NIS-D (UK) | EU NIS Directive/UK NIS Regulations 2018 set out cybersecurity obligations for network and information systems in the critical national infrastructure. | No |
| FINANCIAL | Sarbanes-Oxley Act (SOX) is a federal law for auditing and financial regulations for public companies. | No |
| HEALTH | Health Insurance Portability and Accountability Act (HIPAA) | No |
| CREDIT CARD | Payment Card Industry Data Security Standard. PCI/DSS | No |
| PRIVACY INCLUDING PERSONAL IDENTIFIABLE INFORMATION (PII) | EU GDPR (General Data Protection Regulation) and DPA 2018 (Data Protection Act) | Yes |
| Others | PII data is being handled, and this includes in non-production environments as well. Privacy assessments are being carried out to support this. Also, further discussions are taking place, to ensure that PII data is obfuscated on non-production platforms |  |

## Baseline Security Requirements (BSR’s)

The attached Security Requirement assessment will need to be completed as part of the Requirements Phase in order to establish the level of scope in this area.



## Security Tower Engagement

**RED** = services non-existent

**AMBER** - need to expand services

**GREEN** - services in place and scalable

|  |  |  |
| --- | --- | --- |
| Security Tower | RAG status | Comments |
| Business Partnership & Integration | **GREEN** |  |
| BP&I – Technology Standards | **GREEN** |  |
|  |  |  |
| Physical Security | **GREEN** |  |
| Vulnerability | **GREEN** |  |
| Identity & Access Management | **GREEN** |  |
| Data Protection | **GREEN** |  |
| Platform Security | **GREEN** |  |
| Network Security | **GREEN** |  |
| Security Orchestration Automation and Recovery (SOAR) | **GREEN** |  |
| Incident Response | **GREEN** |  |
| Threat - Training & Awareness | **GREEN** |  |
| Threat – Resilience Planning & Preparation | **GREEN** |  |
|  |  |  |
|  |  |  |

# IT Commercial

# Appendix

