**Conceptual Solution Architecture**

**For**

**Workforce Data Domain**

|  |  |
| --- | --- |
| Project Name | Workforce Data Domain |
| INVP # (if known) | INVP 6273 |
| ITLT Sponsor | Bala Lakshmanan |
| IT Business Partner | Lauren Van Der Kolk Caroline |
|  |  |
| Lead Solution Architect  Data Architect | Shemshuddin Mohammed  Harsh Mundel |
| Infrastructure Architect | { Enter value } |
| Security BP&I /  Security Architecture | Michael Dean  { Embed email sign-off as evidence from security team } |

**Document Control**

Classification Internal

Owner

Author

Creation Date: 15/09/2021

Version 0.1

Status DRAFT

Location Architecture Group Site

Template version v2.14

Replace all fields in Blue on this page, and in tables below

Delete all guidance text in red boxes

**Contents:**

1 Business Vision 3

1.1 Business Context 3

2 Business Scenarios 3

3 Stakeholders and their Concerns 3

4 Constraints 4

5 Business Architecture 5

6 Users and User Experience Expectations 6

6.1 In Scope User Personas 6

7 Current State 7

7.1 Technical Debt 7

8 Risks, Assumptions, Issues and Dependencies 8

9 High Level Solution Architecture 9

10 Technology Disposition Implications 10

10.1 Proposed Introduction of New Technology 10

10.2 Proposed Retirement or Replacement of Technology 10

10.3 Proposed use of Contained / Decommission Technology 10

11 Integration Architecture 11

12 Information Architecture 11

13 End User Compute Architecture 11

14 Cloud & Hosting Infrastructure Architecture 11

14.1 Cloud & Hosting Infrastructure Demand Planning 11

14.2 Capacity Scaling Plan 12

15 Infrastructure / Network Architecture 12

16 Performance Requirements 13

17 Backup Requirements 13

18 Disaster Recovery Requirements 13

19 Technology Risk and Security Architecture 13

19.1 Technology Risk 13

19.2 Information Classification / Criticality 14

19.3 Regulatory Impacts 14

19.4 Baseline Security Requirements (BSR’s) 16

19.5 Security Pattern 16

19.6 Security Tower Engagement 16

19.7 Additional Security Patterns 17

20 Operating Model 18

20.1 Design to Operate 18

21 IT Commercial 19

# Business Vision

As a part of the WDD project, to support operational improvements and enable the digital transformation, National Grid has the ambition to build a data-driven enterprise, which in turn requires Human Resources (HR) to assume the role of Workforce Data Domain Owner

* **Deliver workforce data in the enterprise data platform** -
* **Organise** **people, process and technology** to support efficient use of data and harness the full value potential, we do things one way globally.
* **Develop our maturity**\**capabilities** and empower users to exploit data in the best value-adding way.
* Deliver **golden record and a persistent global worker id** inside a strategic MDM platform as part of MVP 1.

## Business Context

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

Tactical MDM, tactically delivered a 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.

As a part of WDD in MVP1 we deliver **golden record and a persistent global worker id** inside a strategic MDM platform

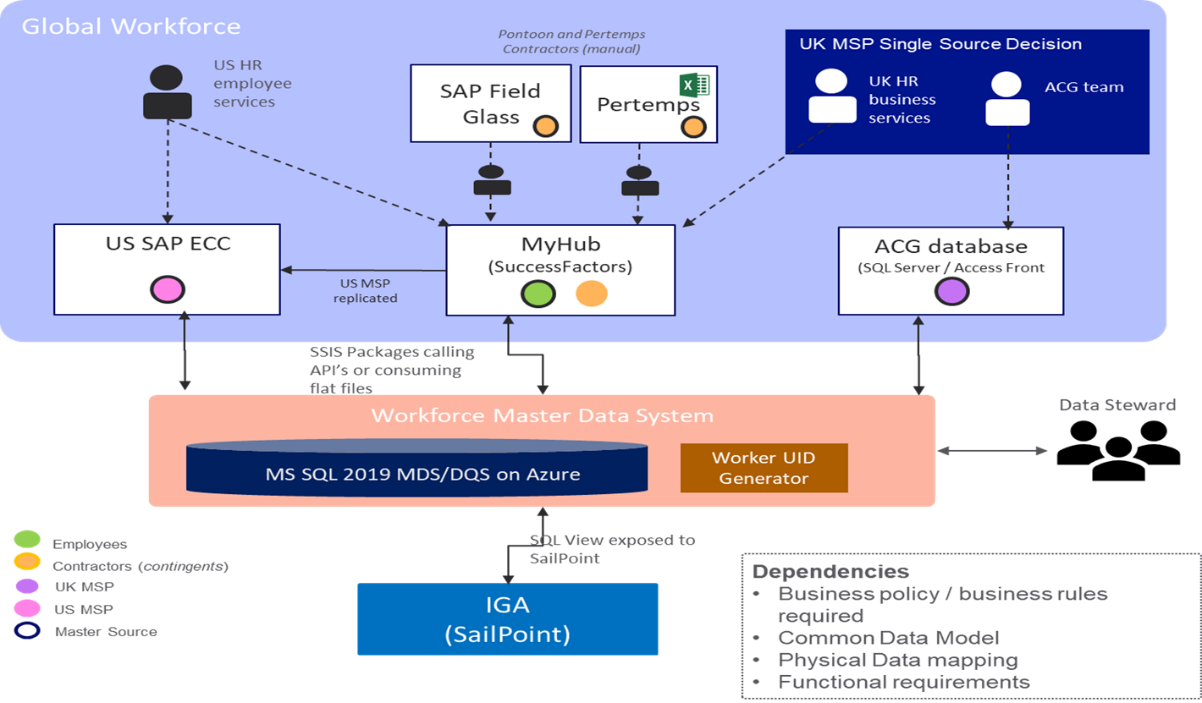
The current use case is the IAM processes requires a unique worker id to be provided to SailPoint.

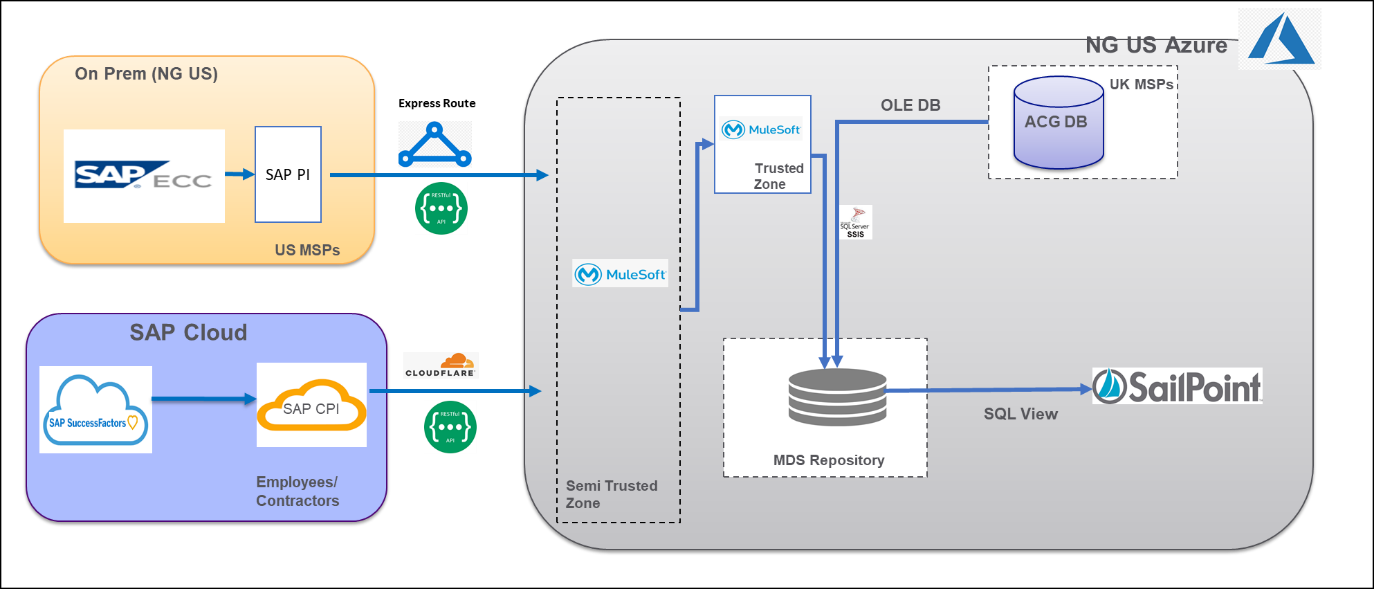
\*The workforce data domain is notable in that it has by far the greatest number of ‘integrations’ to downstream systems or vendors that need to consume data about our workers. This data is used for critical functional processes – keeping our workforce safe, scheduling our workers to keep the lights on, removing access to our critical systems when workers leave our organisations, paying the pensions, salaries and taxes of employees. We have over 120 data integrations to downstream systems Keeping our workforce engaged, enabled and motivated relies on our capability to deliver a domain that is:

* Accurate – the data inside the domain can be relied upon, it is always right. Currently, we consume a large amount of manpower fixing or amending defective as well as spending excessive time gaining assurance that the data is right before committing it to a process.
* Consistent – There are more than 120 integrations built which consume data from the same systems. However, since most of these integrations were built as part of individual projects, the output may not be consistent. Each of these integrations has assumed a certain model. This project will establish a golden record and establish a central platform and share the data with all the downstream systems, thus ensuring consistency.
* Digitally scalable – the platforms that secure and transmit our data are modern and fit for purpose. New consumers can connect to the data cheaply, securely and quickly meaning we get to 'democratised data' where it is more accessible to the business in a better / more efficient way?
* Cost competitive – the costs of running the domain are significantly less than the benefits we obtain from enabling our functional processes and being able to make fast data-driven decisions

**Current State:** The following diagram shows the 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)





The TO BE state in MVP1 will be to replace the Tactical MDM solution with Reltio and provide the data feed from Reltio to Sailpoint.

The data feeds from MY Hub, US ECC and ACG will be sent to Reltio and then Reltio will send the Golden ID record to Sailpoint. Section 5 outlines the details of MVP1 Scope

# Business Scenarios

The following are the business scenarios covered:

|  |  |  |
| --- | --- | --- |
| Worker Type | End to End Process | Sub-Process |
| Employee | Join to leave  HR | Compensation & Global Reward |
| Job Architecture |
| HR Admin – Employee Central |
| Exit Management |
| Analytics & Workforce Planning |
| Reporting |
| Inclusion & Diversity |
| Recruitment |
| Onboarding & Cross-boarding |
| Talent & Succession |
| Performance Management |
| Development Planning |
| Learning |
| Source to Pay  Procurement | Source to Hire |
| TBC | Contingent/Contractor Worker data Admin |
| MSP Worker Data Admin |

# Stakeholders and their Concerns

HR business services UK and the US are the key stakeholders in the WDD program:

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

**1 - Poor Data & information Governance.**

**2 - Poor Data Assurance & Controls**

**3 - Limited Data Processes / Standards**

**4 - Lack of visibility of the data to drive insights**

**5 - Misinformation / no standards terminology or ownership**

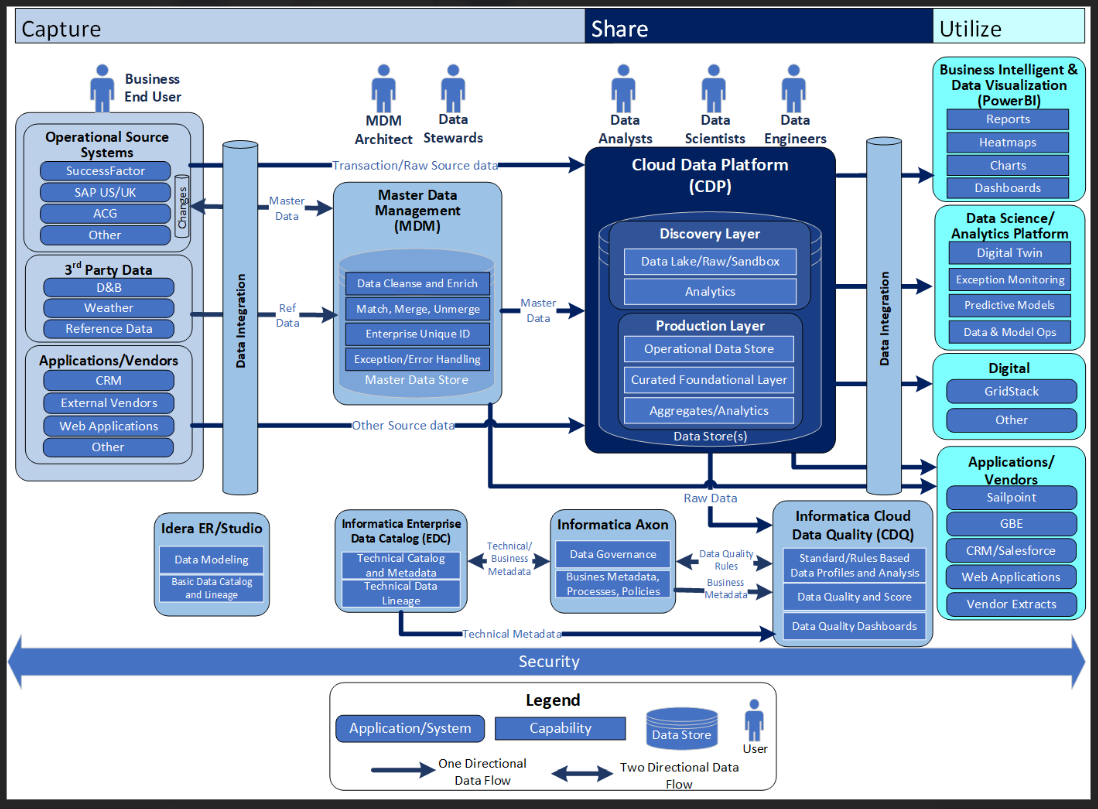
# Constraints

The current constraints are:

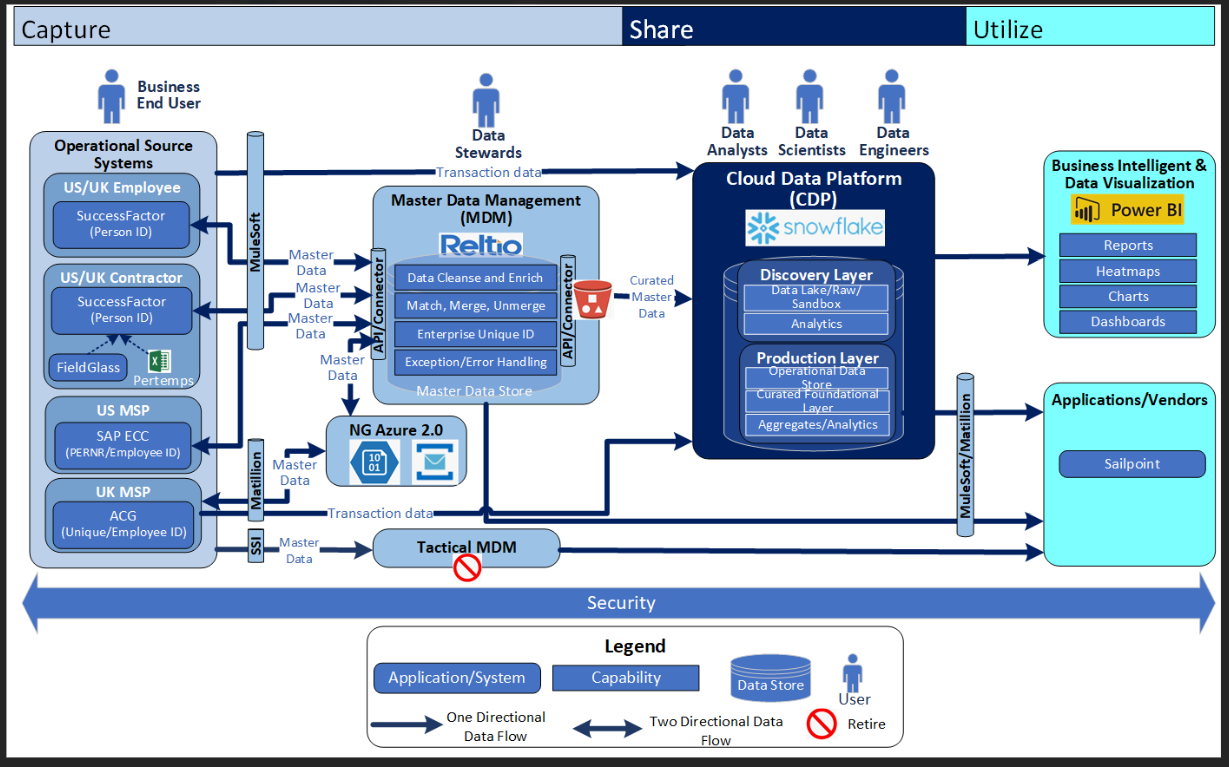
Timeline of MVP1

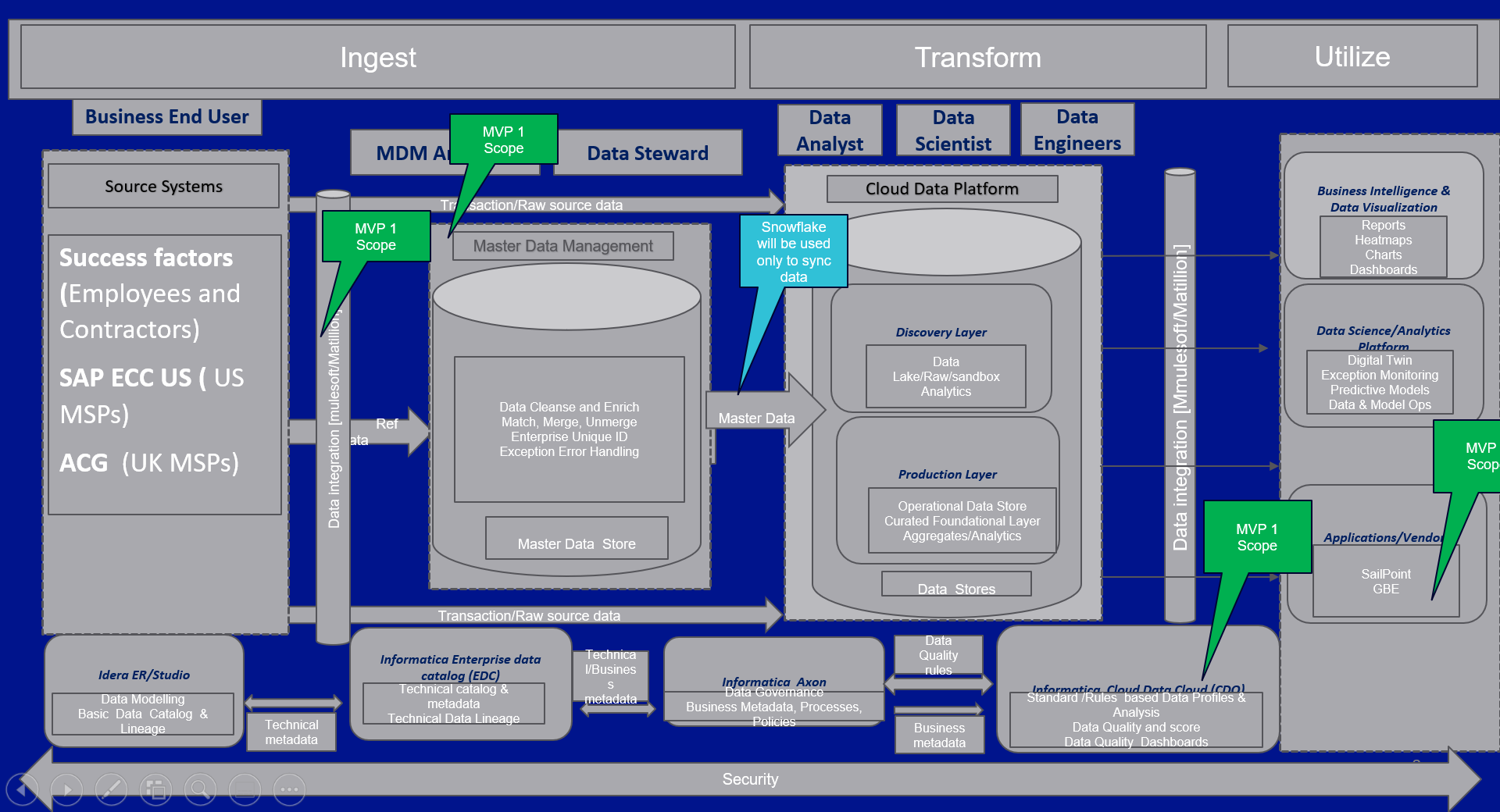
Dependency of source systems SAP ECC, SAP Success Factors on On Boarding and EC modules

# Business Architecture



**MVP1 SCOPE marked**





Components & Scope

#Reltio – Master Data Management

#Mulesoft – Integration Tool

#Matillion – Integration tool

#Informatica – Data Quality

**The scope of MVP1**

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.

As a part of WDD in MVP1 we deliver golden record and a persistent global worker id inside a strategic MDM platform

The current use case is the IAM processes requires a unique worker id to be provided to SailPoint.

**Note: As a part of MVP 1 the following connectivity patterns are Work in progress:**

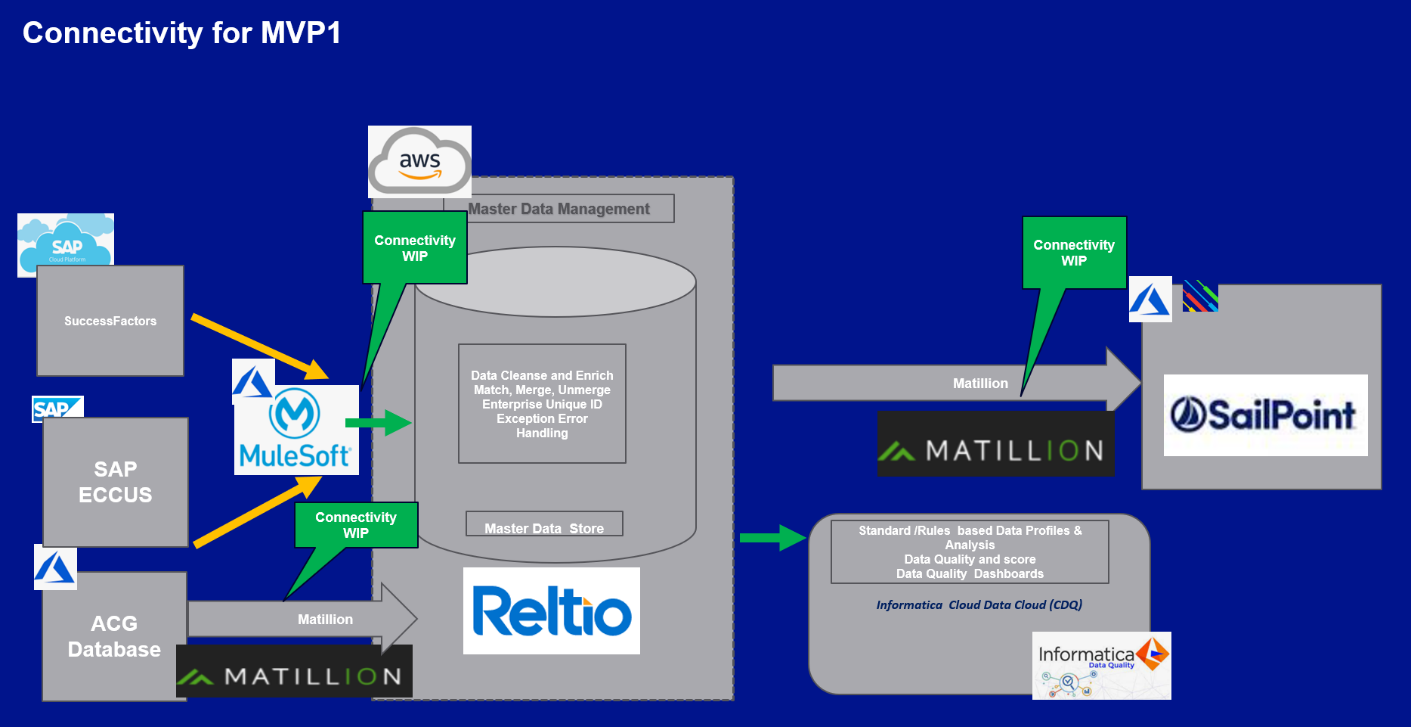
Data Residency discussion along with correct TOMs for handling the data ( Work in progress)

Comparing the Matillion vs Mule Integration patterns (POC with Matillion - Abbas Ali / Mallik SAP)

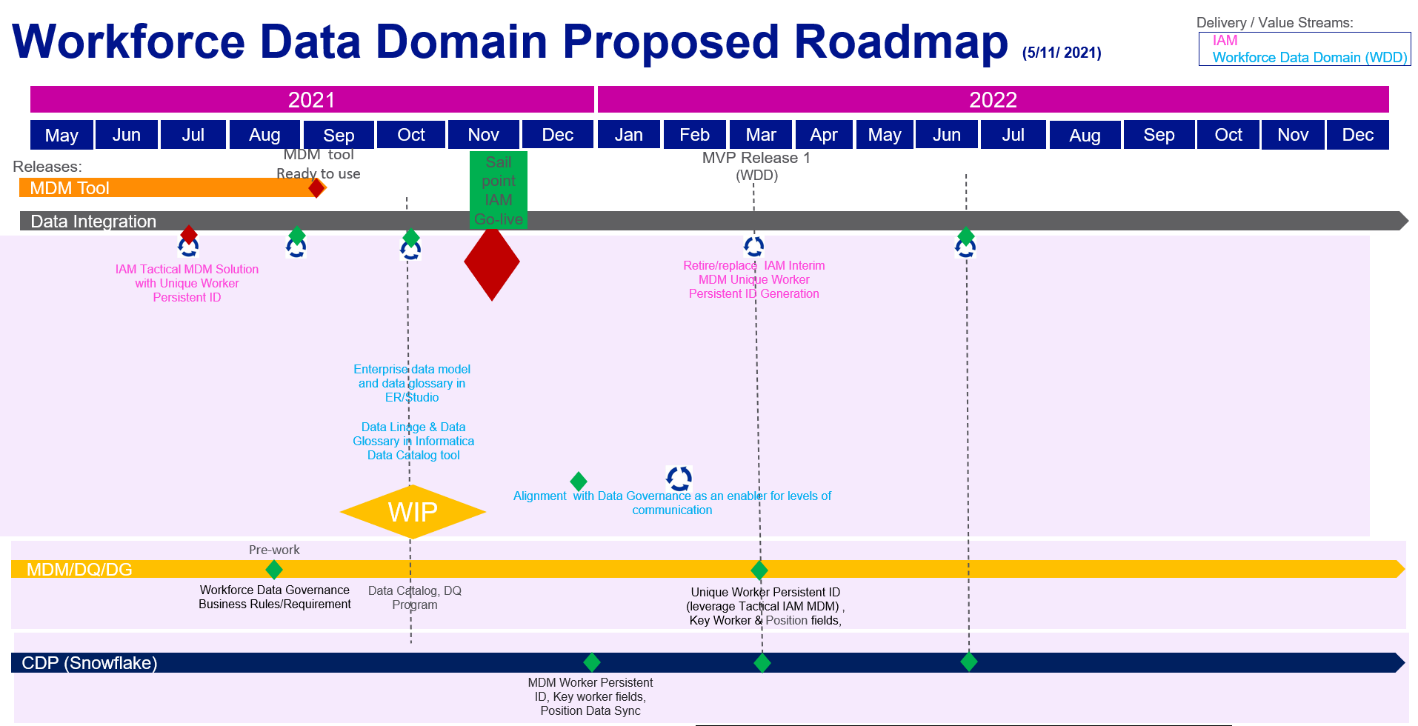
Logical Data Model - WIP (Information Architecture section)

Connectivity between the following components: in progress

* Mulesoft to Reltio
* ACG to Reltio
* Reltio to Sailpoint through Matillion (This is a new connectivity pattern and it’s yet to be discussed with Security)



**Roadmap View of MVP1**



# Users and User Experience Expectations

{ Enter Text }

{

The purpose of this section is to define the user and user experience expectations.

This section is mandatory for any scope including user (including administrative) access.

}

## In Scope User Personas

|  |  |  |
| --- | --- | --- |
| Persona | Interacting Internal/External  to Corp Network | User Impact or User Expectations |
| Field Engineer |  |  |
| Supervisor |  |  |
| Customer |  |  |
| Office Based Worker |  |  |
| Mobile Worker |  |  |
| Privileged / Admin users |  |  |
|  |  |  |

# Current State

The following diagram shows the 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,

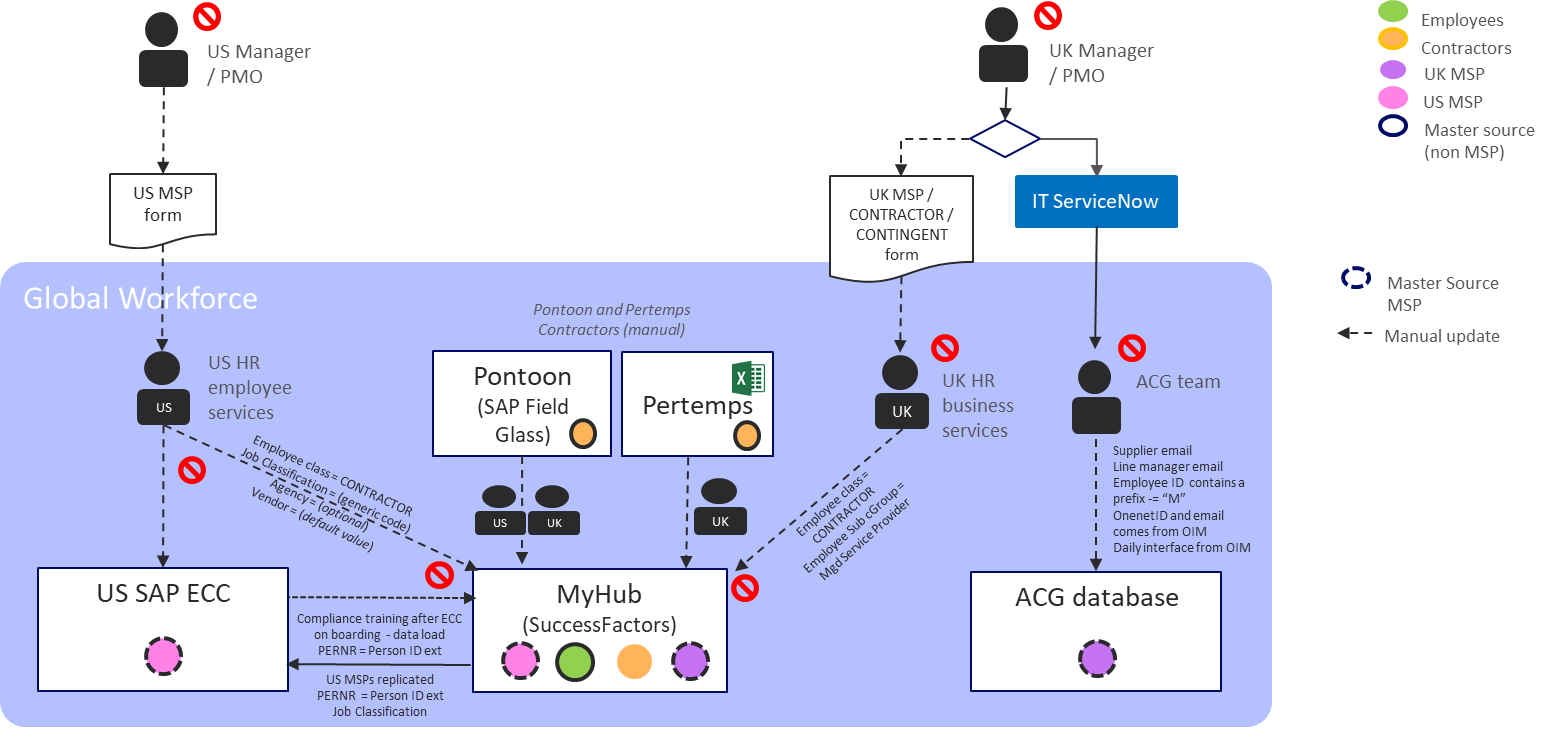
the unique worker ID (Golden record) will be generated which will then be sent across to IAM (SailPoint)

* Employees and Contractors data will be sent from SuccessFactors system to the MDM via the SAP CPI middleware
* The data from the SuccessFactors would be transferred via SAP CPI to the MuleSoft Platform over a secured rest-based API call
* MuleSoft API will invoke the stored procedures from the SSIS packages of the MDM and submit the data to MDS repository
* Only the incremental records will be pulled from the SuccessFactors
* The records would be pulled for every 4 hours

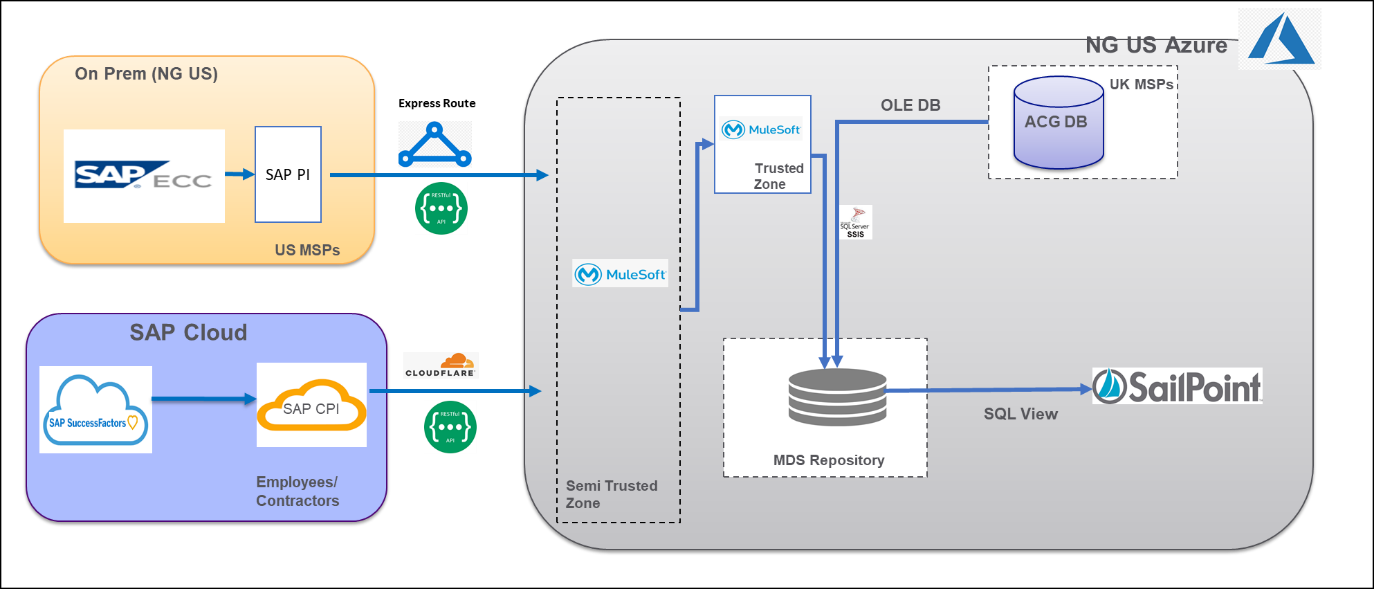
The workforce data for MDM will be obtained from the following 3 source systems

* + - 1. Success factors – Employee & contingent/contractors + Learning module data
      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 (section 13.3.1) will be applied to the records to identify the Golden record with unique worker id which will then be sent to the IAM (SailPoint) system



Current State:

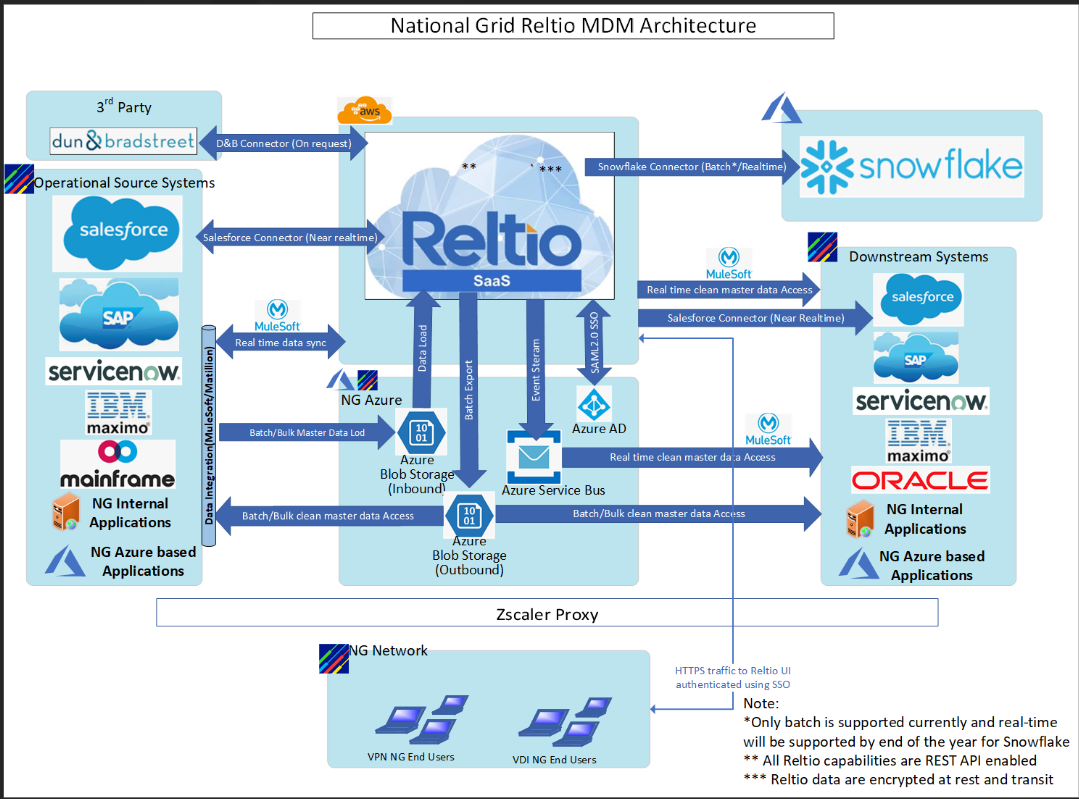


## Technical Debt

# Risks, Assumptions, Issues and Dependencies

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | Type | Risk / Assumption / … | Mitigation | Severity | Likelihood |
| 1 |  | There is risk that there will be an impact of MyHR2.0 on WDD | Regular connects with MYHR2.0 team to mitigate any impact of change at Source |  |  |
| 2 |  | There is a risk that changes to sources like SAP ECC, SAP SF will change the Attribute extraction patterns and the extraction logic may have to rewritten | Regular connects with MYHR2.0 team to mitigate any impact of change at Source |  |  |

# High Level Solution Architecture



# Technology Disposition Implications

{ Enter Text }

{

Referring to the Technology Reference Model (TRM), describe what technologies are required to deliver the service. Highlight any new or non-standard technologies which will be used, and / or any technologies removed from the estate.

The Technology Reference Model (TRM) is at [**<TRM>**](https://nationalgridplc.sharepoint.com/sites/GRP-INT-Architecture/Shared%20Documents/General/Z.%20Archived%20Documents/EA%20Master%20Data/TRM)**[[1]](#footnote-2)**

**Where a project impacts an entry in the TRM – the project must ensure that the appropriate changes are communicated to Enterprise Architecture.**

This section is mandatory.

}

## Proposed Introduction of New Technology

|  |  |  |
| --- | --- | --- |
| Technology  (Application Name) | Capability  (L3) | Rationale |
| 8.5.1 Data Warehouse | Snowflake | <Example> |
|  |  |  |

## Proposed Retirement or Replacement of Technology

|  |  |  |
| --- | --- | --- |
| Technology  (Application Name) | Capability  (L3) | Rationale |
|  |  |  |
|  |  |  |

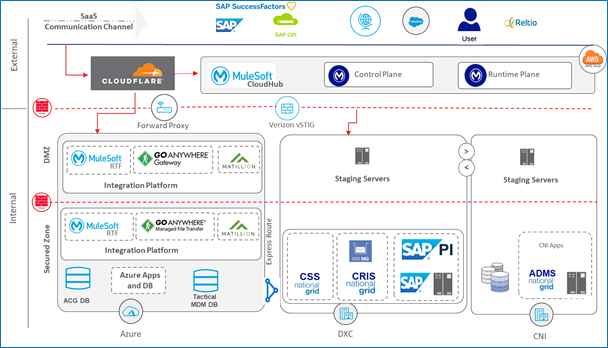
## Proposed use of Contained / Decommission Technology

|  |  |  |
| --- | --- | --- |
| Technology  (Application Name) | Capability  (L3) | Rationale |
| 8.5.1 Data Warehouse | MongoDB | <Example> |
|  |  |  |

# Integration Architecture

High Level E2E Integration Platform

Below architecture diagram shows the E2E Integration of Distributes applications. The architecture covers all possible integration scenarios:



|  |  |  |
| --- | --- | --- |
| **TYPE** | **SCENARIO** | **INTEGRATION PLATFOM** |
| **External – External** | SaaS Application/Public Cloud Apps to Other SaaS or Cloud Apps | MuleSoft CloudHub |
| **External – Internal (DXC)** | SaaS Application/Public Cloud Apps to Applications hosted in On-premise DXC Data centres | MuleSoft RTF (REST APIs)  GoAnywhere (File Transfers) |
| **External – Internal (CNI)** | SaaS Application/Public Cloud Apps to Applications hosted in On-premise CNI Data centres | MuleSoft RTF (REST APIs)  GoAnywhere (File Transfers) |
| **External – Internal (Azure)** | SaaS Application/Public Cloud Apps to Application hosted in NG Azure | MuleSoft RTF (REST APIs)  GoAnywhere (File Transfers) |
| **Internal (DXC) – Internal (DXC)** | Applications hosted in On-premise DXC Data centres | MuleSoft RTF (REST APIs)  GoAnywhere (File Transfers) |
| **Internal (DXC) – Internal (CNI)** | Applications hosted in On-premise DXC Data centres to Applications hosted in On-premise CNI Data centres | MuleSoft RTF (REST APIs)  GoAnywhere (File Transfers) |
| **Internal (DXC) – Internal (Azure)** | Applications hosted in On-premise DXC Data centres to Applications hosted in NG Azure | MuleSoft RTF (REST APIs)  GoAnywhere (File Transfers) |
| **Internal (Azure)- Internal (Azure)** | Between Applications hosted in NG Azure | MuleSoft RTF (REST APIs)  GoAnywhere (File Transfers) |

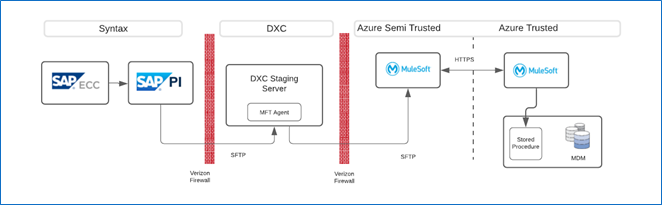
Cloudflare is common gateway for all external applications integration with NationGrid application hosted in Azure, DXC or CNI.

E2E Security will be aligned to the defined BSR guidelines. For details about how security security implemented for Integration services, please refer the confluence link:

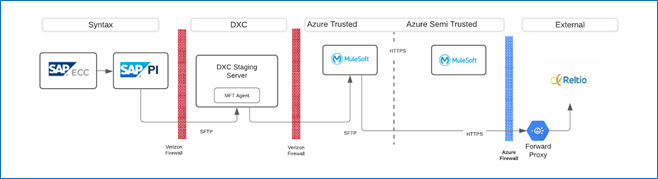
<https://confluence.us.ngridtools.com/display/INT/Security+Framework>

## Integration Scenario#1: SAP ECC to MDM:

Tactical MDM Solution (already in production)



MVP1 Solution



**Alternate Option:** In case SAP PI support API based call outs, PI can directly call Reltio API to load the data.

**Open Point to discuss:**

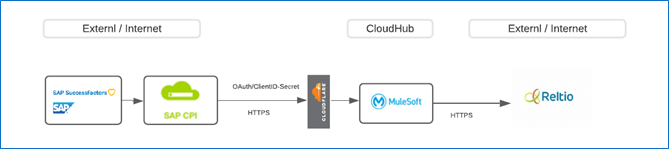
* Transaction type supported by Reltio – Bulk or record by record?
* One time and change data load volume

|  |  |
| --- | --- |
| **#** | **Integration Summary** |
| **1** | The US MSP records will be sent from US SAP ECC to the MDM via SAP PI middleware |
| **2** | The data from SAP ECC would be transferred via PI to the Staging server hosted in DXC through secured FTP channel. MuleSoft platform over a secured rest API |
| **3** | MuleSoft will pick the file from staging server and read the content |
| **4** | MuleSoft will then invoke the stored procedures from the SSIS packages of the MDM and submit the data to MDS repository |
| **5** | Only the incremental records will be pulled from the US SAP ECC |
| **6** | The records would be pulled for every 4 hours |
| **7** | Post successful data load to MDS repository, file will be archived at DXC staging server |

**Error Handling:**

In case the file is not parsed properly during load to MDS repository, email notification will be sent out and file will not be archived from DXC staging server. Production support team will work to re-process the file

## Integration Scenario#2: SAP CPI to MDM



**Open Point to discuss:**

* Transaction type supported by Reltio – Bulk or record by record?
* One time and change data load volume

|  |  |
| --- | --- |
| **#** | **Integration Summary** |
| **1** | Employees and Contractors data will be sent from SuccessFactors system to the MDM via the SAP CPI middleware |
| **2** | The data from the SuccessFactors would be transferred via SAP CPI to the MuleSoft Platform over a secured rest-based API call |
| **3** | MuleSoft API will invoke the stored procedures from the SSIS packages of the MDM and submit the data to MDS repository |
| **4** | Only the incremental records will be pulled from the SuccessFactors |
| **5** | The records would be pulled for every 4 hours |

## Integration Scenario#3: ACG to MDM

ACG to MDM integration will be done through Matillion ETL tool. No Mulesoft or GoAnywhere will be used for this case.

Note: For all mule related integration we are conducting an additional POC to figure out whether Mattillion or Mule is the best fit from a strategic perspective.

# Information Architecture

# End User Compute Architecture

{ Enter Text }

{

Describe the end-user compute requirements for the solution, including:

* Thick-client GUI
* Remote access GUI (VDI / RDP / Citrix etc)
* Mobile UI
* Browser UI (including browser requirements / limitations, and / or desktop / mobile requirements)
* Management UI (in addition to main user UI)

If applicable, include input from infrastructure Architecture

}

# Cloud & Hosting Infrastructure Architecture

{ Enter Text }

{

Describe the server and storage requirements for the solution (include estimated server numbers / storage capacity (including backup) for each hosting type Public Cloud / Private Cloud / CNI Data Centre) and summarise the relevant solution architecture.   
Describe the set of environments that will be deployed (Dev / Test / Prod etc)

Include input from infrastructure Architecture

Include service level requirements

}

## Cloud & Hosting Infrastructure Demand Planning

{ Enter Text }

{

Summarise any key outputs from review of the [Cloud & Hosting Infrastructure Capacity Demand](https://nationalgrid.service-now.com/ksp?id=ksp_cat_item&sys_id=d4ee537e1b3078106c45b886d34bcb93) SNOW request.

}

## Capacity Scaling Plan

{ Enter Text }

{

Describe whether, or not, the solution will grow over time; if it will grow, summarise the factors which will influence that growth, and the time horizon for the change (and what growth capacity is included in the initial deployment).

Consider growth factors such as: data retention, adding users / customers / sites etc

}

# Infrastructure / Network Architecture

{ Enter Text }

{

Describe the network requirements for the solution and summarise the relevant solution architecture.

Include input from infrastructure Architecture

}

# Performance Requirements

{ Enter Text }

{

Describe the performance requirements and related architecture.

Where detailed non-functional requirements (NFR) are not yet defined, summarise the areas of NFR to be addressed and approach.

}

# Backup Requirements

{ Enter Text }

{

Describe the backup requirements and related architecture

Cover separately backups, virtual machine snapshots and data archiving as applicable.

}

# Disaster Recovery Requirements

|  |  |  |
| --- | --- | --- |
| Element | Value | Source / Justification |
| Recovery Time Objective (RTO) |  |  |
| Recovery Point Objective (RPO) |  |  |

{ Enter Text }

{

Describe how the RTO / RPO non-functional requirements will be met.

Describe the high-level approach DR / High Availability / High Resilience / No DR; automatic / manual failover etc.

Describe any project specific architecture solution to provide DR.

If applicable, summarise any Business Contingency Plan (BCP) which mitigates against the need for DR.

}

# Technology Risk and Security Architecture

{ Enter Text }

{

This section to be developed by project Solution Architect, Security Architecture and BP&I Security Integration Lead

However, we expect Security contributions to be throughout all sections where the information is relevant and contextual.

Security is not confined to just this section.

}

## Technology Risk

{ Enter Text }

{

Identify below any key Technology Risk Control Categories applicable to this solution.  Then describe how any critical controls not addressed elsewhere in this document will be met.

If necessary, contact the Program & Project Risk Assurance (PPRA) Mail: [DL.PPRA@nationalgrid.com](mailto:DL.PPRA@nationalgrid.com).

This section is mandatory.

}

|  |  |  |
| --- | --- | --- |
| 1. Cyber Security | 1. Physical Security | 1. IT Resilience |
| Awareness & Training | Physical Security | Backups |
| Incident Response | Personnel Security | Business Continuity |
| Continuous Monitoring | Facility Security | Disaster Recovery |
| Risk Mgmt & Assessment | 1. **IT Operations & Perf Management** | 1. **Supply chain** |
| System Logging | Asset Management | Service Level Agreements |
| Threat & Vulnerability Mgmt | Change Management | System & Services Acquisition |
| Access Control | Config Management | 1. **Data Management** |
| Identification & Authentication | Capacity, Avail & Perf Mgmt | Data Security |
| Cyber Security Management | Patch Management | Privacy |
| Security Architecture | Problem Management |  |
| Network Security | System Maintenance |  |

## Information Classification / Criticality

{ Enter Text }

{

Highlight which Information classifications /criticality levels for this solution needs to support (which in turn informs what controls are required)

Refer to [BSR: NET-2 Network Zone Selection](https://nationalgridplc.sharepoint.com/sites/GRP-INT-US-SecurityBusinessPartneringIntegration/BPI/NET-2%20Network%20Zone%20Selection.aspx?csf=1&web=1&e=c9YwIl&cid=75b74bbd-0a65-41c3-bc5a-4d5ae2fcb339) and [Data Management BMS Standard](https://gridhome.nationalgrid.com/documents/sppreview/d93c6be7-9c01-4ea9-9ee5-bbf864947a3b).

}

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 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 |  |
| CRITICAL ELECTRIC (ENERGY) INFRASTRUCTURE INFORMATION (CEII) | US regulation covering specific engineering, vulnerability, or detailed design information about proposed or existing critical infrastructure |  |
| NIS-D (UK) | EU NIS Directive/UK NIS Regulations 2018 set out cybersecurity obligations for network and information systems in the critical national infrastructure. |  |
| FINANCIAL | Sarbanes-Oxley Act (SOX) is a federal law for auditing and financial regulations for public companies. |  |
| HEALTH | Health Insurance Portability and Accountability Act (HIPAA) |  |
| CREDIT CARD | Payment Card Industry Data Security Standard. PCI/DSS |  |
| PRIVACY INCLUDING PERSONAL IDENTIFIABLE INFORMATION (PII) | EU GDPR (General Data Protection Regulation) and DPA 2018 (Data Protection Act) |  |
| Others | TBC |  |

NOTE: Data Residency discussion along with correct TOMs for handling the data ( Work in progress)

Data Classification: Confidential

## Baseline Security Requirements (BSR’s)

{ Enter Text }

{

Insert the BSRs into this document section from the BSR [folder](https://nationalgridplc.sharepoint.com/:f:/r/sites/GRP-INT-Architecture/Shared%20Documents/Security%20Domain/Baseline%20Security%20Requirements?csf=1&e=XGjPRp).

Working with the Security / Solution Architects, identify the asset types and associated requirements that apply to the project and complete the details in the last two columns.

Include additional security requirements beyond the BSRs based on the known business and non-functional requirements as needed

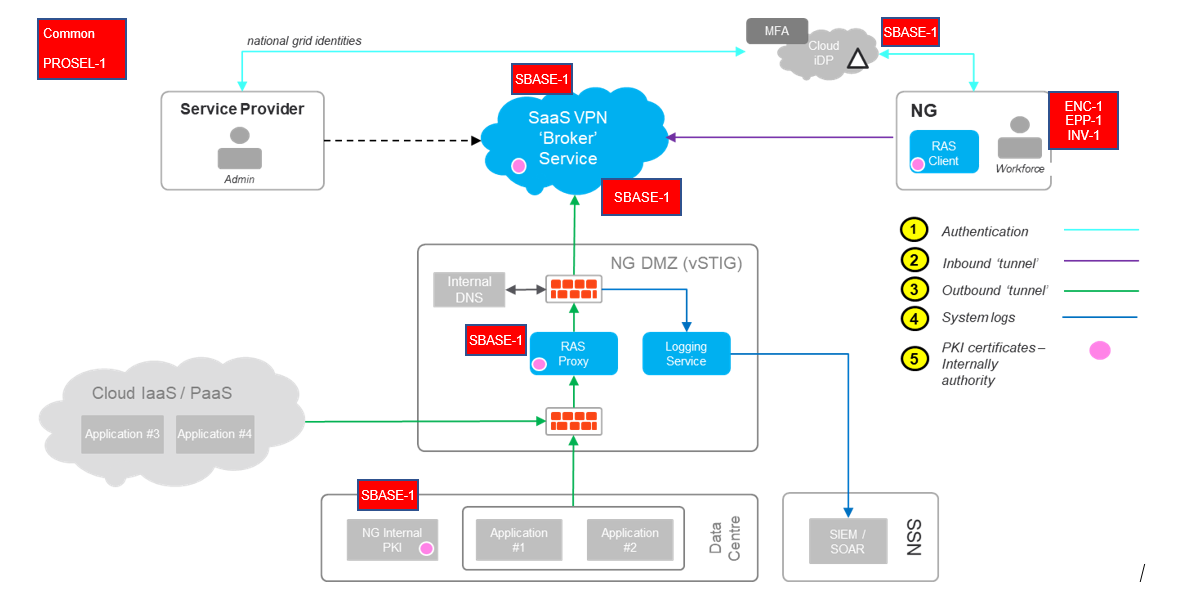
}

## Security Pattern

{ Enter Text }

{

A pattern view of the target conceptual architecture, overlaid with BSR controls / references - example pattern:

  
  
}

## Security Tower Engagement

{ Enter Text }

{

For each Security Tower confirm level of architecture / service impact to the current security service offerings. Leverage the [Capabilities Model](https://nationalgridplc.sharepoint.com/:f:/r/sites/GRP-INT-Architecture/Shared%20Documents/Security%20Domain/2.%20Security%20Capability%20Model%20and%20Standards?csf=1&e=KGj3e8) to identify the applicable services that will be included in the design and list in the table below for each Product area. Include new, proposed services if a gap in existing services has been identified.

}

**RED** = services non-existent

**AMBER** - need to expand services

**GREEN** - services in place and scalable

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

## Additional Security Patterns

{ Enter Text }

{

For known controls where patterns are published and to be reused

Examples include:

* Identity and Access Management
* SOAR / SIEM
* Vulnerability Management
* EPP / EDR

}

# Operating Model

{ Enter Text }

Describe the proposed operating (support) model for the solution, including:

* Does the solution require a new support capability?
* Does the solution have significant Run-The-Business (RTB) costs?
* How does the support model align with the RTO / RPO?

If applicable, include input from Service Transition / Service Owner

## Design to Operate

{ Enter Text }

{

This section to be developed by project Solution Architect and Service Transition Analyst

However, we expect Design to Operate considerations to be throughout all sections where the information is relevant and contextual.

Design to Operate is not confined to just this section.

}

|  |  |  |
| --- | --- | --- |
| Requirement | Compliance | Justification |
| The solution is designed to be resilient at both infrastructure and application layer | Complies  Partial  N/A  Unknown |  |
| The service monitoring requirements are defined and can be implemented in standard NG strategic operations tools | Complies  Partial  N/A  Unknown |  |
| Solution is scalable with minimum component change. | Complies  Partial  N/A  Unknown |  |
| All component of solution has established support arrangements | Complies  Partial  N/A  Unknown |  |
| Accurate and well baselined Run The Business costing model to include full and end to end total cost of ownership including and not limited to support contract costs, licensing costs, service management costs. | Complies  Partial  N/A  Unknown |  |
| All Starter movers and leavers requirements are considered for the solution | Complies  Partial  N/A  Unknown |  |
| All the applicable service support activities from list below are considered and documented for proposed solution   * OS Support Services, * OS Patching, * Database Management, * Event Management, * Storage Management, * Backups, * Restoration, * Backup monitoring, * Capacity Management, * Network Management * Data Protection at Rest (Encryption) | Complies  Partial  N/A  Unknown |  |

# IT Commercial

{ Enter Text }

{

Input from IT Commercial

* What are the commercial implications of this architecture?
* Do we need new licenses? Do we need services?

}

1. At the time of updating this template there is no full export of TRM to Physical Technical Component export from Alphabet, if necessary, use the most recent TRM and TC Template from the TRM/Archive folder. [↑](#footnote-ref-2)