

T-Level Results and Certification

Architecture Design Pack

December 2019

Created by: Nick Fribbens & Sam Kirsten

Contents

[1 Logical design 4](#_Toc27734168)

[1.1 Problem statement 4](#_Toc27734169)

[1.2 Goals and drivers 6](#_Toc27734170)

[1.3 Stakeholder / Location and Actor Viewpoints 7](#_Toc27734173)

[1.4 Design Principles 8](#_Toc27734174)

[1.5 High-level solution concept view 9](#_Toc27734175)

[1.6 Business Context Viewpoints 12](#_Toc27734176)

[1.7 Data Architecture 17](#_Toc27734177)

[1.7.1 Data Sources 20](#_Toc27734178)

[1.7.2 T Level Data Definition 21](#_Toc27734179)

[1.8 Design Requirements, Constraints, Risks and Issues 23](#_Toc27734180)

[1.9 Business Requirements 24](#_Toc27734181)

[1.10 Assumptions 25](#_Toc27734182)

[1.11 Constraints 26](#_Toc27734183)

[1.12 Risks 26](#_Toc27734184)

[2 Physical Design 27](#_Toc27734185)

[2.1 Simplified Physical Design 27](#_Toc27734186)

[2.2 Detailed Physical Design with Individual Components 28](#_Toc27734187)

[2.2.1 Physical Design Detail 29](#_Toc27734188)

[2.3 Reusable Components 31](#_Toc27734189)

[2.3.1 Reusability 32](#_Toc27734190)

[2.4 Resources 32](#_Toc27734191)

[2.5 Hosting 34](#_Toc27734192)

[2.6 API design 35](#_Toc27734193)

[2.6.1 API List 37](#_Toc27734195)

[2.6.2 Data Transfers 38](#_Toc27734196)

[2.7 Security 42](#_Toc27734197)

[2.7.1 Data Security 44](#_Toc27734200)

[2.7.2 Threat Model 45](#_Toc27734201)

[2.7.3 Perimeter Security 48](#_Toc27734202)

[2.7.4 Application Security 51](#_Toc27734203)

[2.7.5 Secrets Management 51](#_Toc27734204)

[2.7.6 Monitoring 52](#_Toc27734205)

[2.7.7 Continuous Validation 54](#_Toc27734206)

[2.7.8 PEN Testing Scope – Recommendations 55](#_Toc27734207)

[2.8 Backup, Logging and Audit 58](#_Toc27734208)

[2.8.1 Backup 58](#_Toc27734209)

[2.8.2 Logging and Audit 58](#_Toc27734210)

[2.9 Architectural / Design decisions 58](#_Toc27734211)

[2.10 Data Persistence 59](#_Toc27734212)

[2.11 Document references 60](#_Toc27734215)

[3 Annexes 61](#_Toc27734216)

[3.1 Useful references 61](#_Toc27734217)

[3.2 Glossary of terms 62](#_Toc27734218)

[3.3 Functional requirements 64](#_Toc27734219)

[3.4 Document control 71](#_Toc27734220)

[3.4.1 Expiry or review date 71](#_Toc27734221)

[3.4.2 Version control 71](#_Toc27734222)

[3.4.3 Document approval 72](#_Toc27734223)

# Logical design

## Problem statement

Based on the recommendations of the Sainsbury Review, the Post 16 Skills Plan, published in July 2016, set out the Government’s plan to reform technical education, moving to a simplified system based on routes to employment with T Levels as a flagship qualification. The core purpose of T Levels is to prepare learners for direct entry into skilled employment (including higher level apprenticeships), and therefore will be rigorous, classroom based technical study programmes. Past attempts to reform technical education, particularly 14-19 Diplomas, tried to create qualifications that were both academic and technical to meet requirements of employers and universities, and didn’t achieve either.

The new T Levels will be delivered in subjects including construction, creative and design, digital, engineering and manufacturing, and health and science, with the first T Levels being introduced in September 2020. A T Level digital service will help to support the roll-out of the qualifications, achieving several objectives including raising awareness and understanding; facilitating enrolment on the qualifications; enabling providers to source suitable employer placements; and providing timely results and certification to learners.

In October 2018, work began to consider the potential for development of a T Level service to support the users and service actors of the T Level qualifications being introduced in 2020. We commissioned an external consultancy, Methods, to undertake an 8-week discovery to develop a potential vision for the T Levels service, by understanding user and business needs, as well as the current service and policy landscape. This discovery included an initial identification of potential service areas, common touchpoints, and opportunities to share capabilities between the T Levels service and wider ESFA / DfE services.

In March 2019, the Technical Education Reform Board agreed that the scope of T Levels service should extend to three priority service areas:

**Marketing and Communications** whichlaunchedacampaign website for T Levels for learners and parents to:

* Introduce them to T Levels and explain how they work.
* Pitch T Levels as a viable educational route after GCSEs.
* Tell them which T Levels are being launched and when.
* Encourage them to search for local T Level providers and contact them if they’re interested in studying T Levels.

Work is underway to extend the campaign site for employers, so it can:

* Sell the idea of industry placements.
* Encourage them to register interest in offering industry placements.

At this moment in time there are no further plans to expand the capability of this site after the current work is completed.

**Industry Placements Matching** helps employers and providers arrange industry placements, in preparation for T Levels in 2020. ESFA staff use the service to help employers:

* Create opportunities for students to do industry placements.
* Find local providers with suitable opportunities for students.
* Talk to providers about these opportunities.
* Identify where there are not enough providers to fill their opportunities.

**Results and Certification** is the ESFA internal system to:

* Create a register of T Levels.
* Record which Awarding Organisations offer a combination of pathways and Specialisms that make up a TQ.
* Record which providers are approved to run the T Levels that an Awarding Organisation is offering.
* Record learner’s completion and assessments for pathways, specialisms, MARs, IPs, Maths and English.
* Calculate a learner’s T Level result at the completion of their learning
* Print T Level Certificates or Certificates of Achievement.

This document deals with the service for the results and certification printing process for T Levels.

The T Level structure is illustrated below:

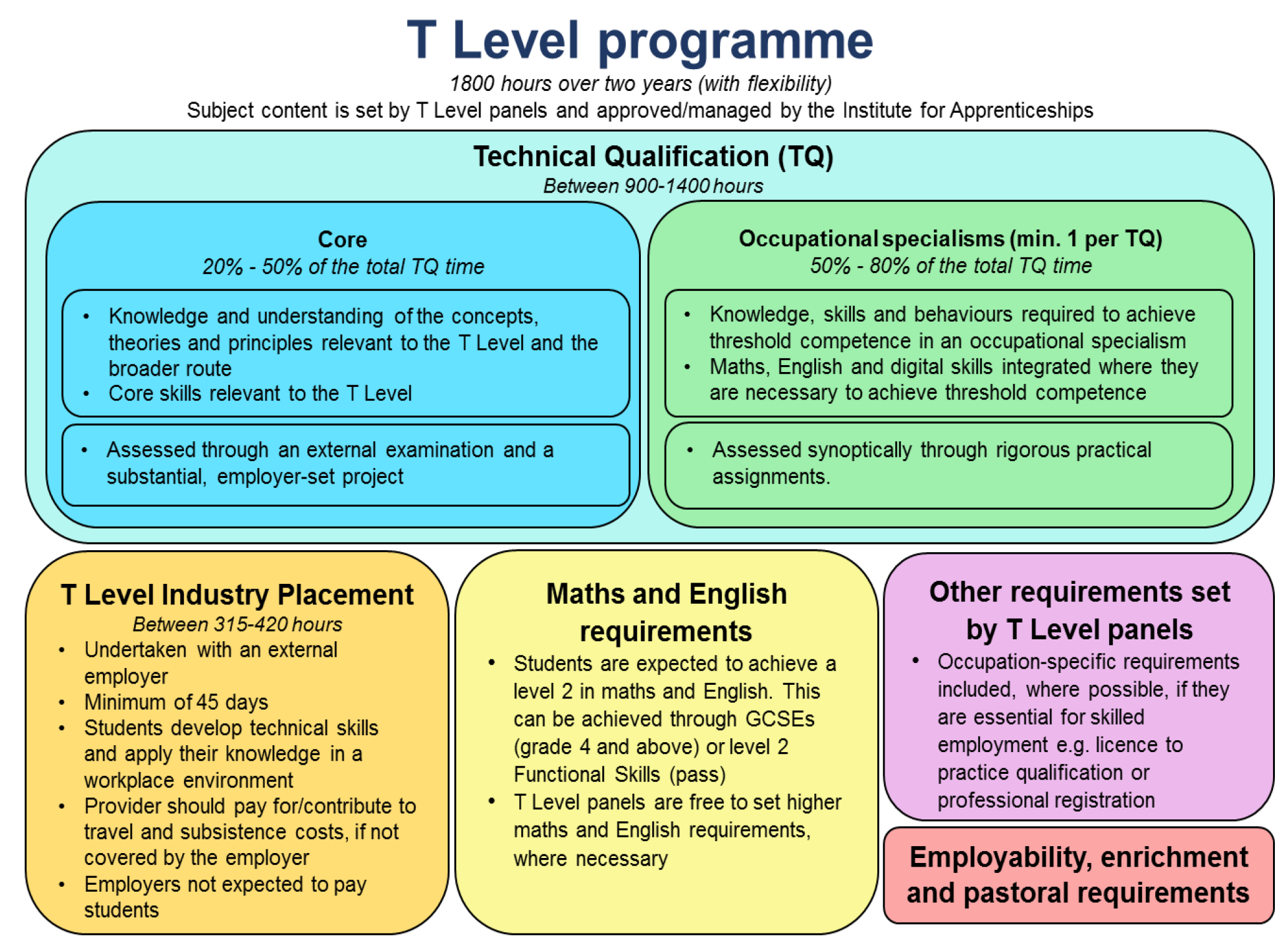


Figure 1 T Level programme definition

## Goals and drivers

T Levels are new courses coming in September 2020, which will follow GCSEs and will be equivalent to 3 A Levels. These 2-year courses have been developed in collaboration with employers and businesses so that the content meets the needs of industry and prepares learners for work.

T Levels will offer learners a mixture of classroom learning and ‘on-the-job’ experience during an industry placement of at least 315 hours (approximately 45 days). They will provide the knowledge and experience needed to open the door into skilled employment, further study or a higher apprenticeship. The Results and Certification system supports the gathering of T Level achievement and the printing of T Level Certificates and Statements of Achievement.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Stakeholder** | **Influence** | **Driver** | **Principles** | **Goal** |
| **ESFA** | High | Government policy | listen  communicate  work | Deliver T Levels |
| **Ifate** | High | Government policy | Communicate | Create T Levels |
| **Awarding Organisation** | Medium | Kudos  Financial | listen  communicate  adopt | Supervise TQs |
| **Provider** | Medium | Kudos  Financial | listen  communicate  adopt | Deliver classroom training  Enable IPs for their learners  Gather Maths, English and MAR attainments |
| **Employer** | Medium | Influence learner training | listen  communicate  adopt | Gain viable employee output  Assess prospective employees |
| **Learner** | Low | Gain qualification for entry into further education or employment | communicate  adopt | Gain a valued qualification |

Table - Goals & Drivers



## Stakeholder / Location and Actor Viewpoints

|  |  |
| --- | --- |
| **Stakeholder** | **Concerns** |
| IFATE | The Institute is responsible for the Technical Qualification (TQ). This is the main, classroom-based element of the T Level, and equips students with the skills and knowledge necessary to give them a broad understanding of their chosen occupational route. |
| Ofqual | Ensure that T-Levels are regulated to provide a consistent quality and that all results of the TQ are recorded as a regulated qualifications |
| DfE | Monitor the take up of T Levels which is the flagship qualification of a simplified system which provides routes to employment. |
| ESFA | Have a concern to provide and monitor T Level funding, but this is not an explicit concern for T Level Results and Certification System. |
| Awarding Organisation | Approve providers to deliver specific TQs, monitor providers performance and record assessment results in preparation for T Level certification calculation. |
| Provider | Provide consistent and measurable T Level education, recruiting learners for their TQs, monitor learner’s completion of their chosen pathways and specialisms and to recruit employers to provide industrial training for their learners. |
| Learner | Ambition to achieve a qualification that is a gateway into both higher education and into future employment |
| Employer | Give employers the chance to ensure that young people are developing the skills and experience that industry needs. |

Table - Viewpoints

## Design Principles

The T Level Results and Certification will adhere to the following design principles:

* Enterprise data will be accessed from an authoritative source rather than duplicated where possible.
* To obliviate storage of redundant data by storing data once in authoritative sources, and retrieving it using common identifiers therefore maintaining referential integrity.
* To use loosely coupled objects with no interdependencies, to ensure that a change made within one object will not create unanticipated changes within other elements. This simplifies testing, maintenance and troubleshooting procedures.
* To reuse common components.

## High-level solution concept view

The diagram below shows how the systems of participating stakeholders interact with one another and the ESFA T Level systems to provide the T Level Results and Certification system.

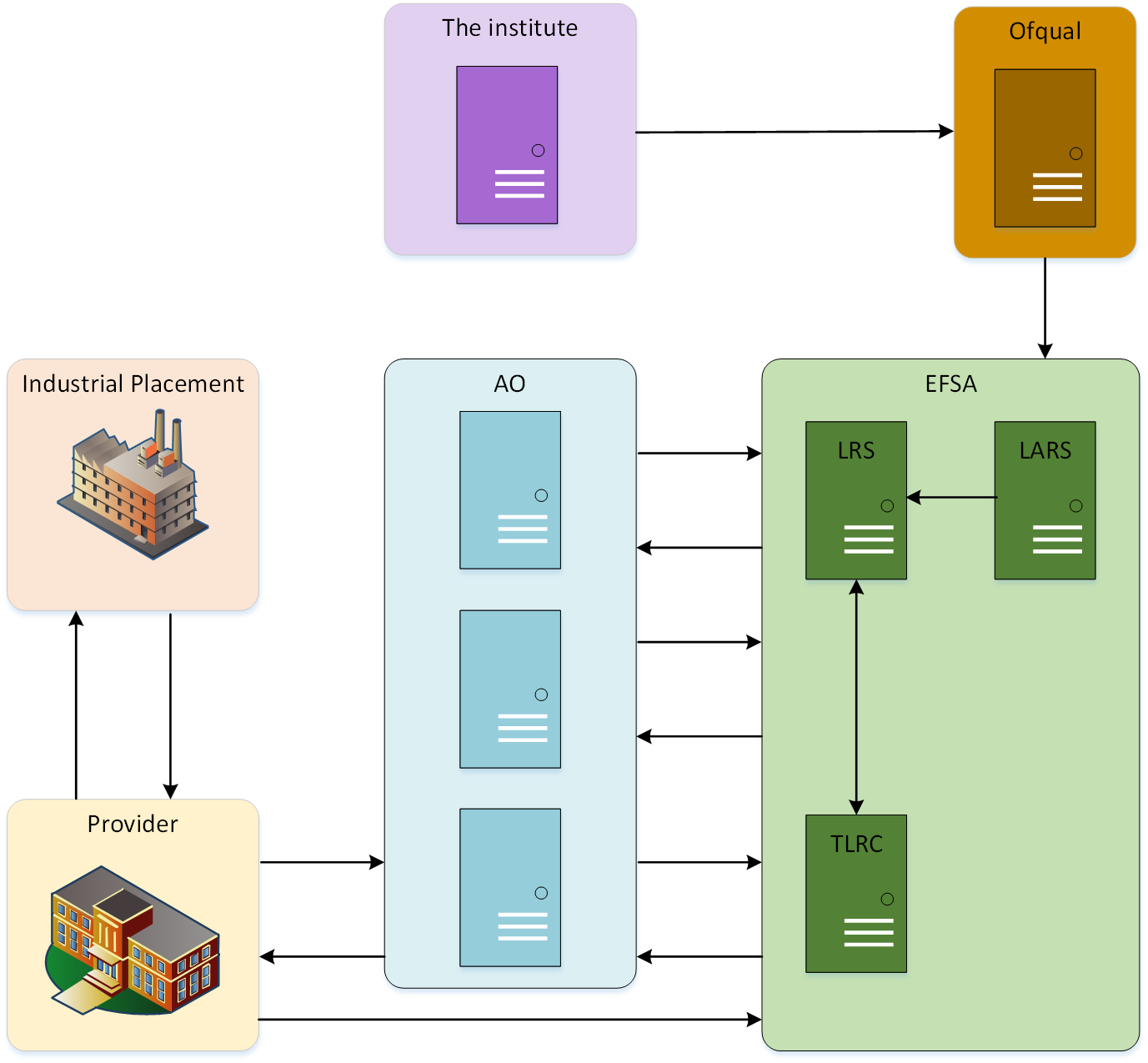


Figure - Organisations

The process begins with Ifate conceiving the T Levels, defining the combinations of pathways together with associated MARS and specialisms to construct a valid TQ combination.

The TQ combinations are passed to Ofqual who in turn take the pathways and specialisms and create regulated qualifications and regulated qualification codes, which are fed into the ESFA system, LARS. LARS in turn updates LRS, to enable LRS to record qualification results against pathways and specialism in the ULR. The 2020 T Level pathways and specialisms are already setup in LRS. A further feed will be sent from Ifate to Results and Certification specifying the TQ constructions of pathways, associated specialisms and MAR requirements.

Learning providers apply to be eligible deliver TQs. Once a provider is eligible it needs to be approved by an AO to deliver the TQ on the AO’s behalf.

The provider then recruits learners for the T Levels it is approved to run. The learner details are stored in the provider’s own systems and passed to AOs, using the ULN,

together with the chosen pathway and specialism information.

AOs store the learner details in their own systems, prior to transferring it to T Level Results and Certification System. Within the T Level Results and Certification System the learner is registered on the specific occurrence of pathways and specialisms with the provided assessment dates, together with the MARs and IP that augment for the pathways and specialisms.

Providers use the ULN to enter the learners’ MARs, IP details together with Maths and English results if not present in LRS for equivalent examinations taken outside England and Wales.

Ten days before the T Level results date the T Level system will trigger a set of emails to be sent to Awarding Organisations and Providers if there are missing assessments or attainments for individual learners.

Seven days before the T Level results date the T Level system will trigger the results calculation for ESFA and will only make the results available to the AOs and providers through LRS at the same time as A Levels.

Prior to the presentation of certificates date, the passed T Level qualification results and details are assembled, together with the associated provider details and sent to the printers, for the T Level Certificates to be printed. The printed certificates are then sent to relevant providers for certificate distribution.

Providers may request a Certificate of Achievement to be printed for learners who have passed T Level components but have not qualified for a T Level.

The final T Level results are available for UCAS to use when learners apply for entry into further education.

This will translate into the solution shown below:

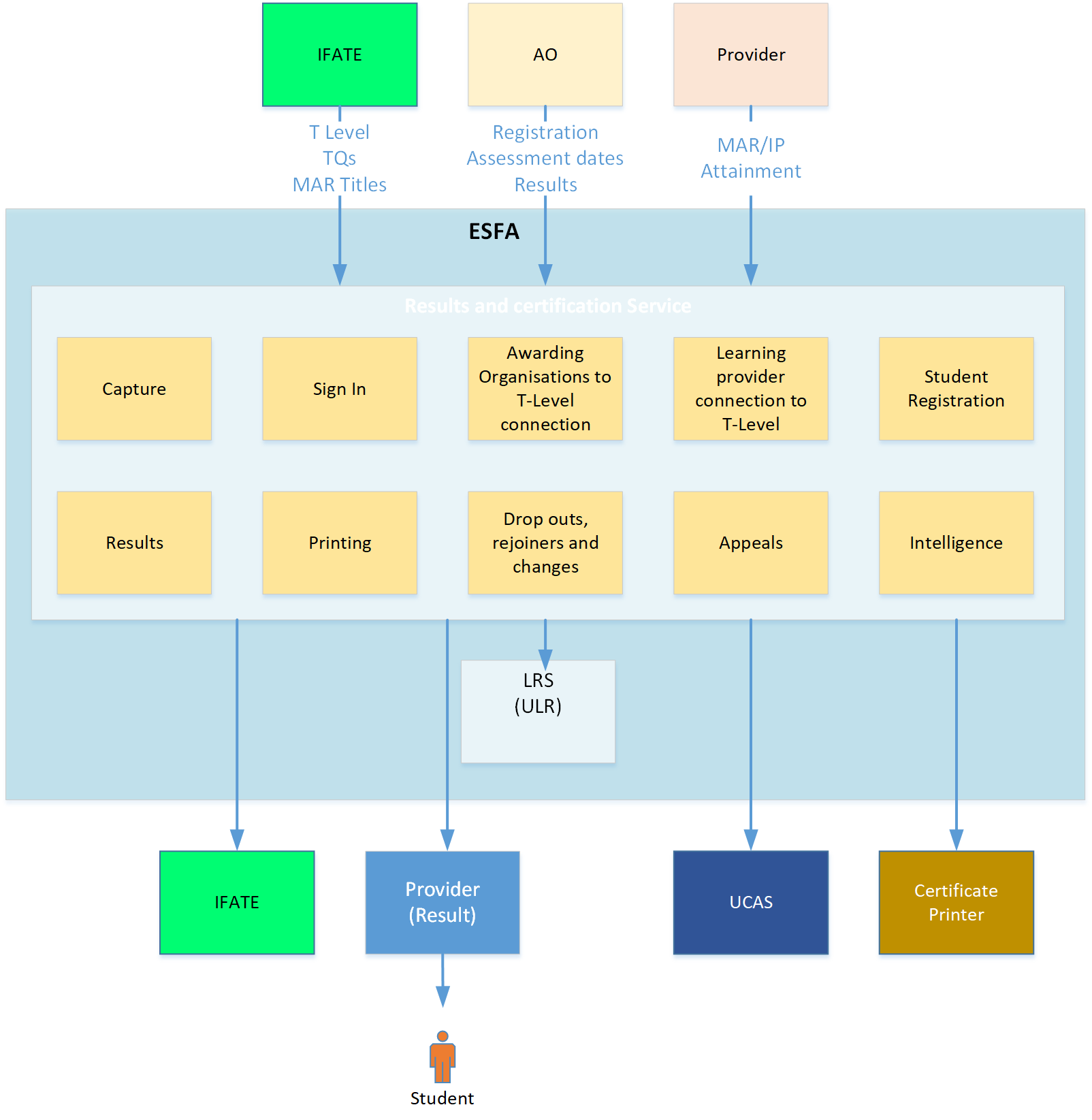


Figure - High-Level Solution Concept

These are the features which are going to be realised in the T Level Results and Certification system. are going to build. The alignment of functions to features is described in [Application to Capability mapping](#_Capability_to_application).

## Business Context Viewpoints

Major functionality will be achieved through the entry of data from third party systems and its integration with internal enterprise data. The collection of data from this disparate data sources will be achieved through system to system interfaces, notably RESTful APIs.

However, not all the organisations required to transfer data to the Results and Certification service will have the resource or capability to create and maintain APIs. To cater for these organisations a portal will be built to enable a file transfer, ie CSV files, to take place or for individual entries to be entered manually or for data to be reviewed by non-technical staff.

To ensure that learner results are entered into the system in a timely manner, reports showing results for learners have not been entered will be sent to the awarding organisations to remind them that there are results that need to be entered.

The diagram below shows the processes which are performed by the main system users.

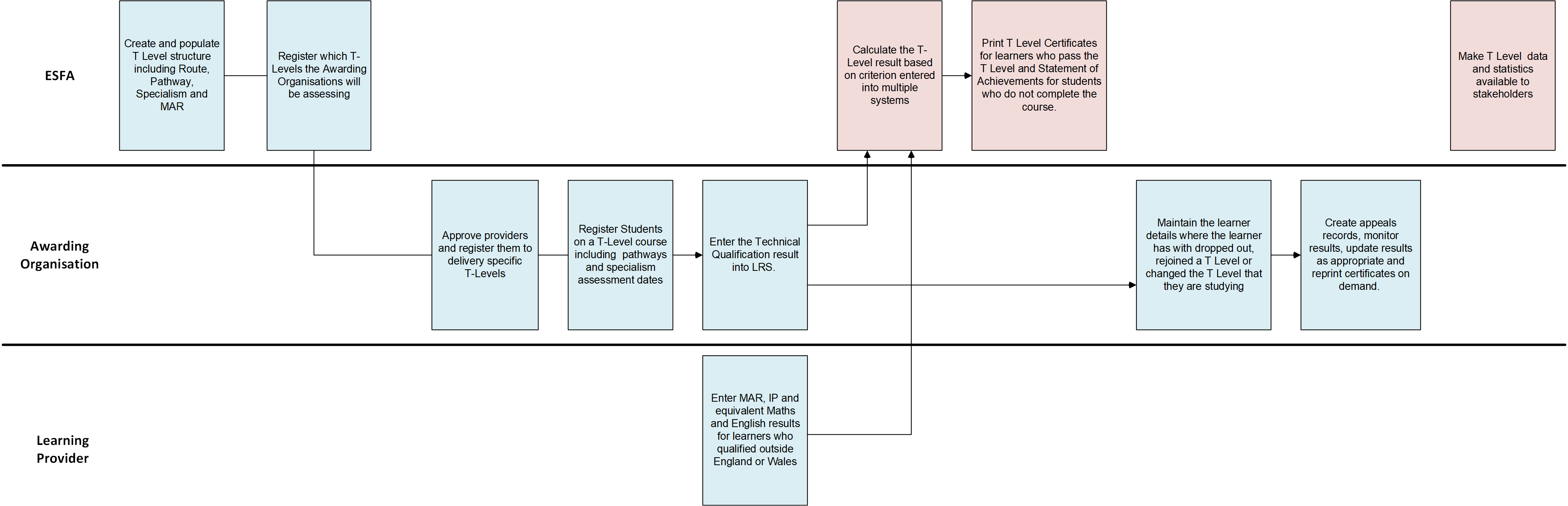
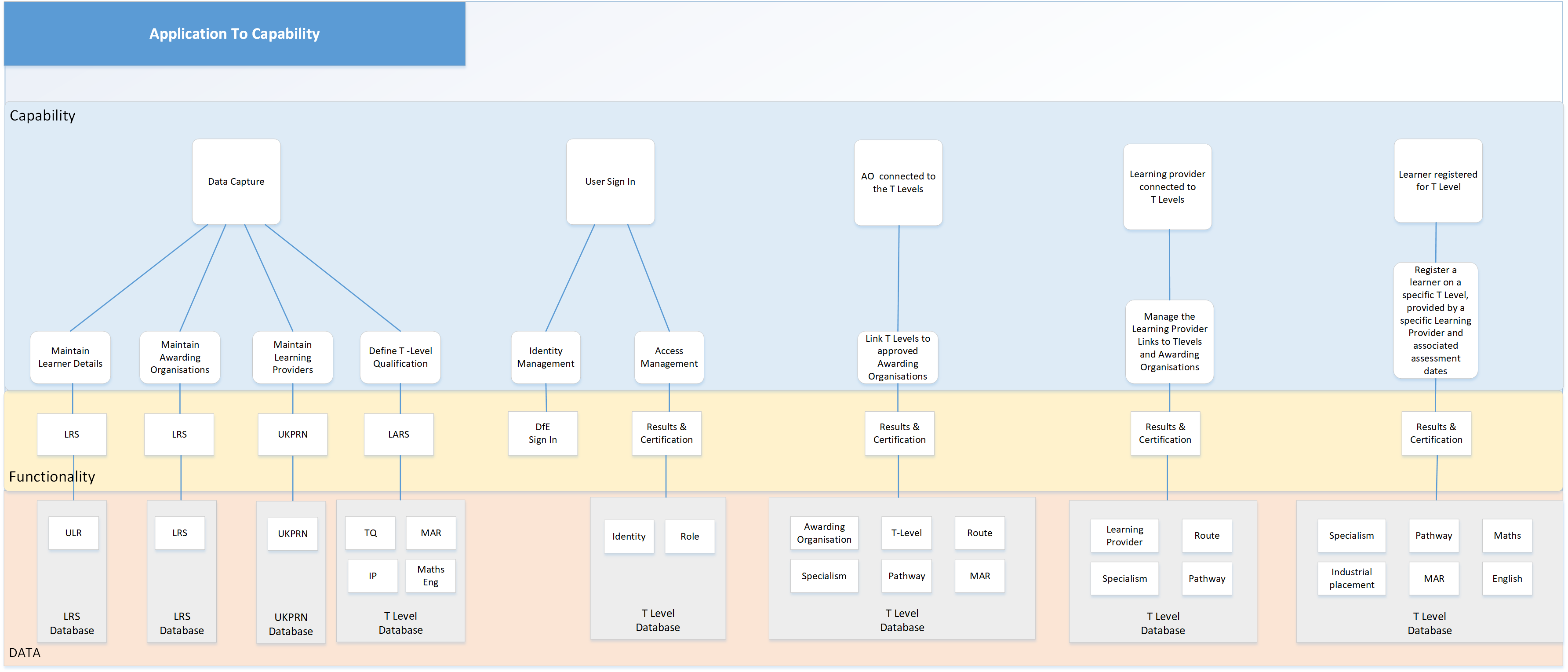


Figure - Swim Lanes for Main Users

The business capability to application map shows the business capabilities with their underlying business process and how these will be mapped to the application functionality.



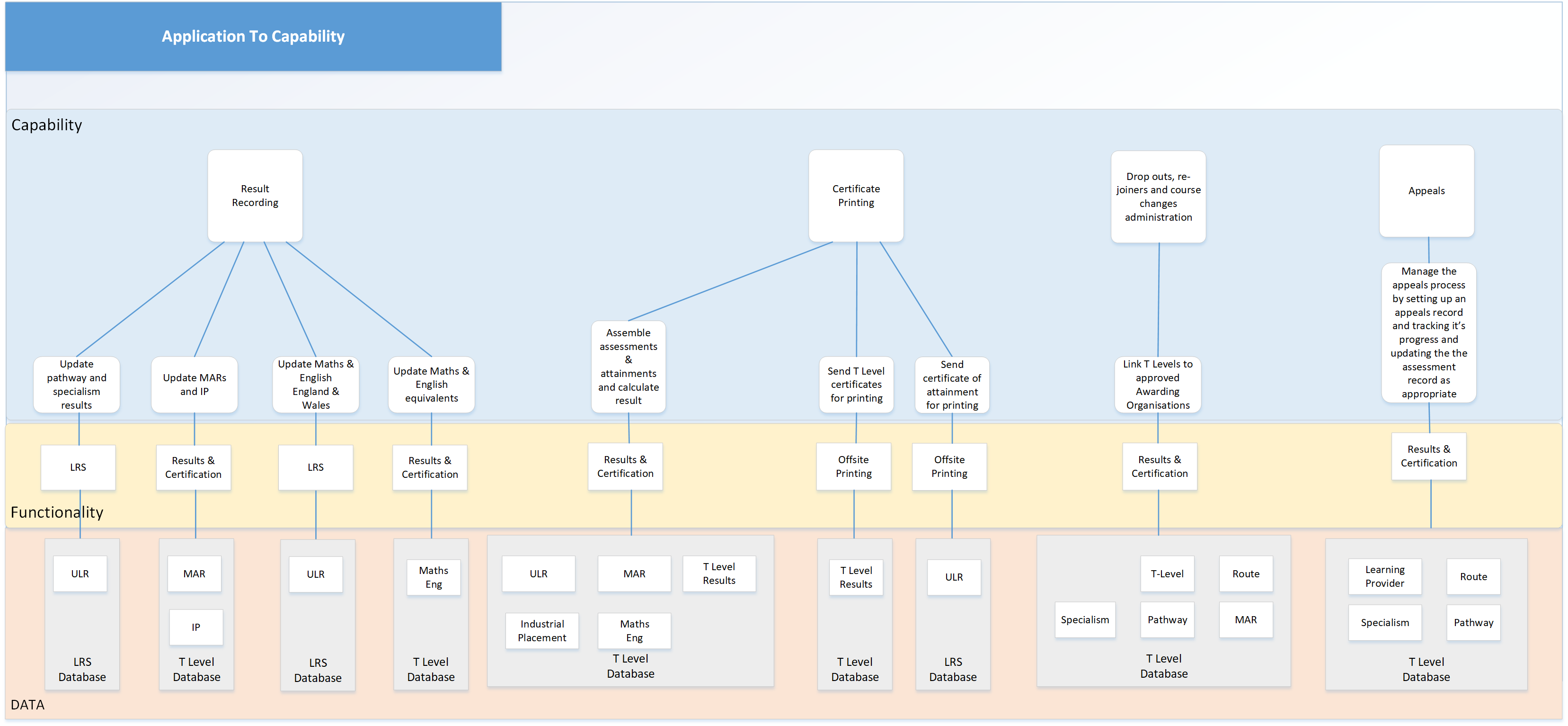


Figure 5 - Business Capability to Application Map

|  |  |  |  |
| --- | --- | --- | --- |
| **Epic ID** | **Epic name** | **Epic description** | **Minimum viable product** |
| E1 | Capture | Providing the ability to store T-Levels in a database including the following attributes, Unique ID, Name, Route, Pathway & Specialism | The T Level database must be defined at field level and implemented  The T Level data, Unique ID, Name, Route, Pathway & Specialism, a will be imported manually from T Level definitions to create TQs structures |
| E2 | Sign-in | Providing functionality for AO's and Providers to sign into the DfE whilst capturing who is signing in and what authorisations they require. | Integrate the T Level Results and Certification System login with the DfE sign-in and create a role-based access management system using Azure RBAC.  Assign user groups to the appropriate roles. Set up policy enforcement points for the management of APIs |
| E3 | Awarding Organisation connection to T-Level | Providing the functionality for IFATE to register which T-Levels the Awarding Organisations will be assessing | The API to allow Ifate to register T Levels to Awarding Organisations will be created The portal to allow Ifate to register T Levels to Awarding Organisations manually will be created Training guides for using both the API and the portal will be created The registering of T Levels to Awarding Organisations will be done manually using the published first year T Level data System documentation |
| E4 | Provider connection to T-Level | Providing the functionality for AO's to advise which provider will which T-Level | The API will be created to allow Awarding Organisations to register which T -Levels, (pathway and specialism), that a Provider will be able to deliver. The portal to allow Awarding Organisations to manually register which T -Levels, (pathway and specialism), Providers will be able to provide to will be created The registering of T Levels to Providers will be done manually using the published first year T Level data Training guides for using both the API and the portal will be created System documentation |
| E5 | Learner registration | Providing the functionality for Providers to register Learners on a T-Level course | The API to allow Awarding Organisations to register learners on T Levels, (pathway and specialism), will be able to provide to will be created The portal to allow Awarding Organisations to manually register learners on T -Levels, (pathway and specialism), Providers will be able to provide to will be created Training guides for using both the API and the portal will be created  System documentation. |
| E6 | Results | Providing the ability to calculate the T-Level result based on criterion entered into multiple systems.    Awarding Organisations enter the Technical Qualification result into LRS.  The provider enters MARs, IP, Maths & English into the Results & Certificates database, and the calculation will then be performed. | Create the APIs to enter pathway and specialism assessments, MAR and IP attainments and the collection of equivalent Maths and English achievements which have been accomplished outside England and Wales.  Create the T Level result calculation, together with the routines and APIs to assemble required the assessment results and associated T Level attainments to calculate T Level results. If there a maths or English achievement is not found in the T-Level database a secondary search will be made in LRS. Training guides for using both the API and the portal will be created  System documentation |
| E7 | Printing | Providing the functionality to print certificates that are accurate, clear, display the correct result and on time.  Functionality will also include Statements of Achievement for learners who do not complete the course. | Create the routines which will assemble the data to be sent to the third-party print provider in order to be able to print T Level certificates.  Provider address details will need to accompany the certificate details in order to deliver the certificates to the location specified by the provider, in order to distribute the certificates on a specified date. The transport mechanism is yet to be decided, as a new print provider is currently being selected. Training guides for using both the API and the portal will be created  System documentation |
| E8 | Drop-outs, re-joiners and changes | Providing functionality for AO's to update the database with leavers, update the database with re-joiners and to make all other necessary changes that may happen | This facility will provide an API to enable the AOs to change the status of a learner to show that they have left a course or are taking a break in studying. The facility will also be available for the learner to change courses or to re-join the TQ they have left within a two year. The functionality provided by the API will be duplicated using the portal. Training guides for using both the API and the portal will be created  System documentation |
| E9 | Appeals | Providing functionality to create appeals records, monitor results, update results and reprint certificates on demand and statements of achievement. | An API will be provided for the AO to use to create appeals records and update the record with the appeal outcome, with the ability to change an assessment score if required. The function will also enable the reprinting of T Level certificates and certificate of achievement if required.  This functionality will be replicated for use via the portal.  Training guides for using both the API and the portal will be created  System documentation |
| E10 | Intelligence | Making data available to all stakeholders | TBD – Potentially mirroring Azure Data Factory on LRS. |

Figure - Epics

## Data Architecture

The T Level system will hold the minimum amount of data required, with links to authoritative sources, which it will retrieve as and when needed. This will remove the need to duplicate the data and ensure that data is accurate.

The T Level Service will hold the data pertaining to T Level descriptions and the pathways and specialisms required to be attained to pass the T Level, together with all mandatory additional requirements and industrial placement completion. Maths and English attainments will be held within the T Level system for all equivalent GCSE attainments which will not be held in LRS.

The system will link the T Level to the awarding bodies who are eligible to award that T Level. In turn, eligible Learning Providers which an awarding organisation has approved to run T Levels will be associated with the awarding organisation and the T Level that the Learning Provider is eligible to run.

The details of the awarding organisations are mastered and held in LRS with the RN number as the unique identifier. When this AO data is required by the T Level system it will be requested from LRS and transferred to the T Level system. There some data items which are pertinent only to T Levels, such as T Level contact email address that will be stored with the T Level Results and Certification System database.

The core provider details will be retrieved the T Level database. In later iterations, this data will be retrieved from UKRLP, the authoritative source using the common identifier, UKPRN. Data that is only pertinent to T Levels, will be stored in the T Level Results and Certification System database, using the UKPRN as identifier. This information will include but not be limited to:

* Applied to deliver TQs.
* Approved to deliver TQs.
* Locations where pathways are delivered, used as the address for the delivery of T Level certificates.
* T Level contact email address.
* T Level results.

The Learner details, such as name and address, will be retrieved from LRS using the LRS APIs when required. This data will be maintained in LRS and will not be held within the T Level system unless required for operations such as printing. This data in LRS will be subject to the current LRS GDPR rules.

Assessment qualifications, MAR and IP attainment cannot be stored for incomplete T Levels for more than two years. Data for learners who have not completed an

assessment for more than two years will be purged from the T Level Results and Certification System.

The results for Pathways and Specialisms assessments will be updated and maintained within the T-Level database as well as LRS, as this is the repository for all a learner’s achievements within the ESFA. To enable the Pathways and Specialisms to have assessments assigned to them, they will need to be set up with Qualification Assessment Numbers. This has already happened as the pathways and specialisms have been created by OFQUAL and transferred to LARS. LARS in turn has forwarded these to LRS.

The calculation of the T Level result will be handled in the T Level system and the result stored within the unique learner record in the T Level database and LRS.

The following diagram shows an ERD that encapsulates the high-level data requirements of the solution and their relationships to other data elements:

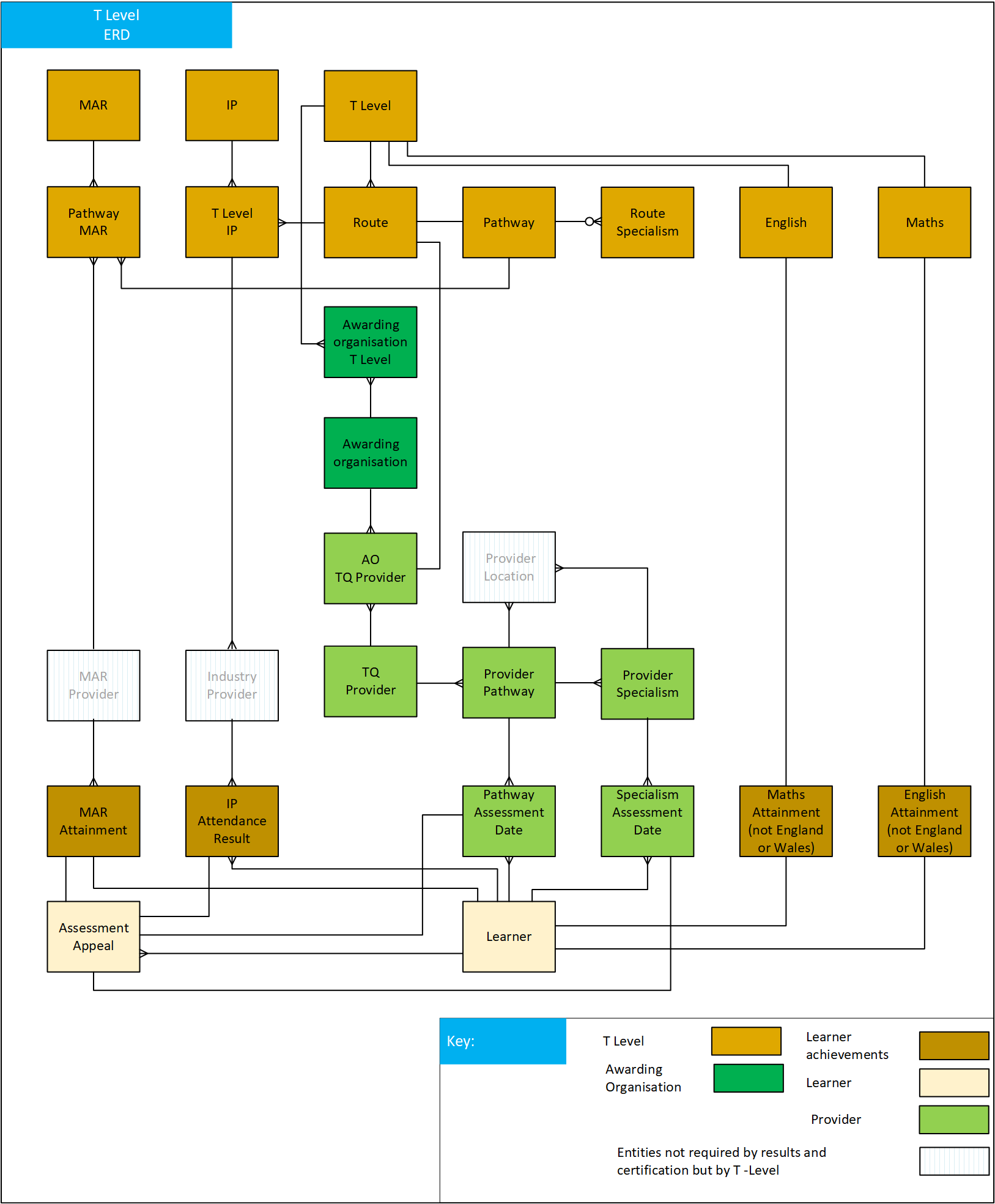


Figure 7 - Entity Relationship Diagram (ERD)

### 1.7.1 Data Sources

| **Data** | **Source** | **Key** |
| --- | --- | --- |
| Learner | ULR | ULN |
| Pathway & results | T Level | ULN, Regulated Qualification Code |
| Specialism & results | T Level | ULN, , Regulated Qualification Code |
| Maths  (England & Wales) | ULR | ULN |
| English  (England & Wales) | ULR | ULN |
| Maths equivalent | T Level | ULN |
| English equivalent | T Level | ULN |
| IP | T Level | ULN |
| MAR | T Level | ULN, Pathway Id |
| Awarding organisation | LRS | RN Number |
| Awarding organisation location pathway | T Level | RN Number  Pathway Id |
| Awarding organisation location Specialism | T Level | RN Number  Specialism Id |
| Learning providers | UKRLP | UKPRN |

Table - Data Sources

### 1.7.2 T Level Data Definition

The following diagram shows the definition of a T Level in data terms, with example data:

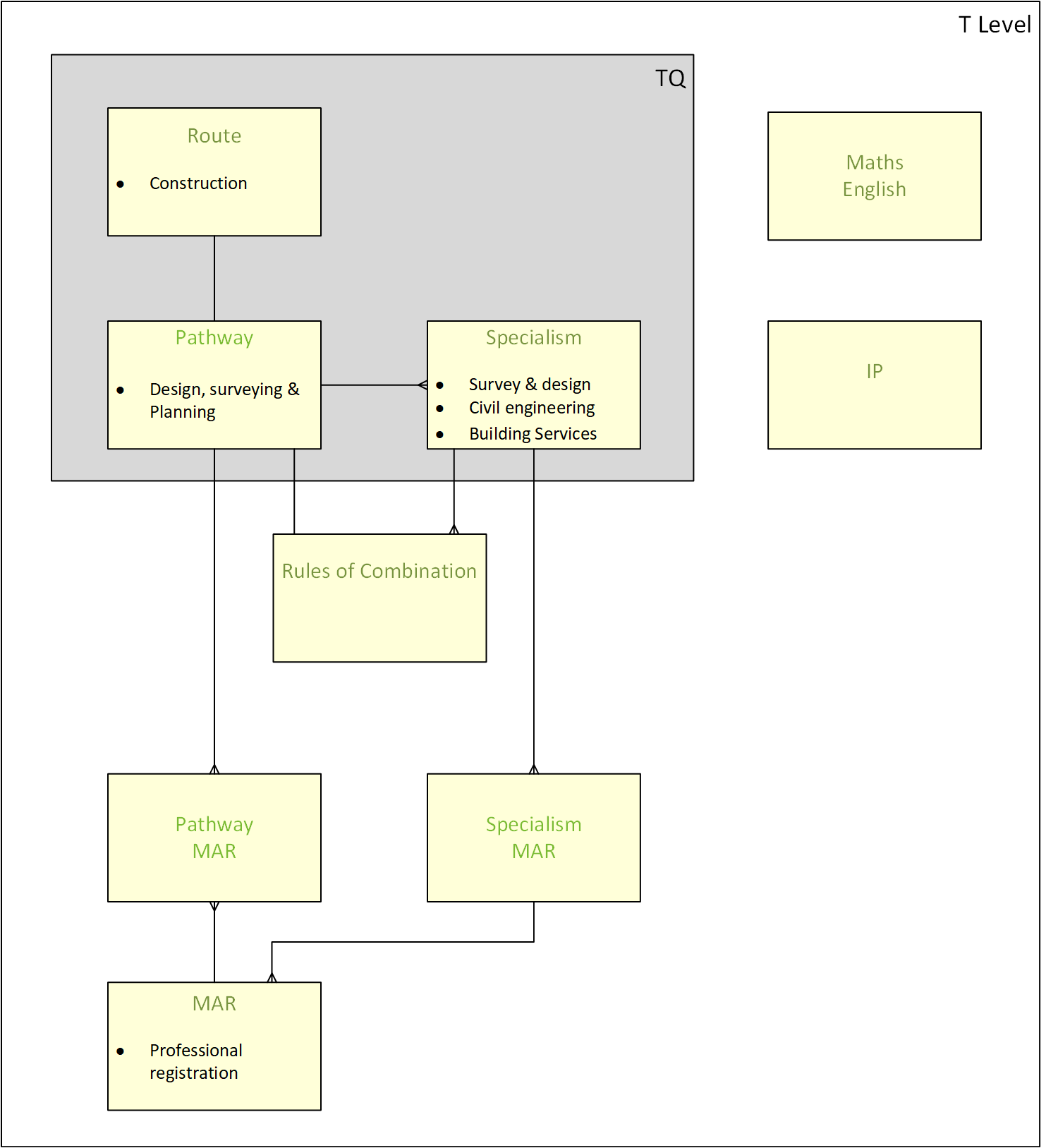


Figure 8 T Level data structure

|  |  |
| --- | --- |
| **Table** | **Description** |
| Route | The Sainsbury Report used labour market information to define 15 technical ‘routes’ to skilled employment. The routes reflect shared requirements for occupationally related knowledge, skills and behaviour. They form the structure through which all technical education will be delivered. |
| Pathway | A pathway is a sub-set of a route which groups common sets of occupations into several occupational clusters. |
| Specialism | The part of the Technical Qualification focussed on developing knowledge, skills and behaviours relevant to an occupation. The time required to deliver and assess each occupational specialism varies depending on how long it will typically take learners to develop threshold competence. A specialism is only associated with one pathway. |
| Pathway Mar | Links a MAR to a Pathway and holds the record as to whether a learner has satisfactorily attained the MAR |
| Specialism MAR | Links a MAR to a Specialism and holds the record as to whether a learner has satisfactorily attained the MAR |
| MAR | A list of all the Mandatory Additional Requirements |
| IP | Industrial placement holds the record as to whether a learner has satisfactorily completed 45 days industrial training. |
| Maths equivalent | The maths record holds whether a learner holds a maths attainment equivalent to a level 2, which does not have a regulated qualification code and is therefore not held in LRS. |
| English equivalent | The English record holds whether a learner holds an English attainment equivalent to a level 2, which does not have a regulated qualification code and is therefore not held in LRS. |

## Design Requirements, Constraints, Risks and Issues

* **Business or technology constraints**
* There is a time constraint from when pathway and specialism results arrive, together with IP and MAR attainment, to enable the calculation of T Level results. If assessments are not received in time the T Level result for the learner cannot be calculated.
* **Significant functional / non-functional requirements**
* Peaks in results arriving, just before A Level results. All T Level assessment and attainment data will be received eight working days before results are due to be released.
* There will be peaks in printing, although not so time critical.
* The system will generate a reminder for Awarding Organisations and Providers for the entry and completion of attainments and assessments.
* Result calculations will be calculated seven working days before the T Level results release date.
* T Level certificate printing will be scheduled to take place at a date yet to be determined.
* On demand T Level certificate and statement of achievement printing will be required for some learners.
* The maximum file sizes for data transferred from Awarding Organisations and Providers has yet to be determined.
* There will be a significant growth in the number of learners taking T-Levels, as follows:
  + 2,300 entrants in 2020
  + 66,500 upon roll-out of all pathways in 2023
  + 120,500 following full national roll-out in 2029

## Business Requirements

|  |  |  |  |
| --- | --- | --- | --- |
| Ref. | Priority | Status | Summary statement |
| BR.01 | Must | Capture | Providing the ability to store T-Levels in a database including the following attributes, Unique ID, Name, Route, Pathway & Specialism |
| BR.02 | Must | Sign-in | Providing functionality for AO's and Providers to sign into the DFE whilst capturing who is signing in and what authorisations they require. |
| BR.03 | Must | Awarding Organisation connection to T-Level | Providing the functionality for IFATE to register which T-Levels the Awarding Organisations will be assessing |
| BR.04 | Must | Provider connection to T-Level | Providing the functionality for AO's to advise which provider will be delivery which T-Level |
| BR.05 | Must | Learner registration | Providing the functionality for Providers to register Learners on a T-Level course |
| BR.06 | Must | Results | Providing the ability to calculate the T-Level result based on criterion entered into multiple systems.    Awarding Organisations enter the Technical Qualification result into LRS.  The provider enters MARs, IP, Maths & English into the Results & Certificates database, the calculation will then be performed. |
| BR.07 | Must | Printing | Providing the functionality to print certificates that are accurate, clear, displays the correct result and on time.  Functionality will also include Statements of Achievement for learners who do not complete the course. |
| BR.08 | Must | Drop-outs, re-joiners and changes | Providing functionality for AO's to update the database with leavers, update the database with re-joiners and to make all other necessary changes that may happen |
| BR.09 | Must | Appeals | Providing functionality to create appeals records, monitor results, update results and reprint certificates on demand. |
| BR.10 | Must | Intelligence | Making data available to all stakeholders |

Table - Business Requirements

## Assumptions

| Ref. | Priority | Status | Summary statement |
| --- | --- | --- | --- |
| A.01 | Must | Assumed | Pathway assessments will be entered directly into LRS using existing services of APIs and portal held in the ULR |
| A.02 | Must | Assumed | Specialism assessments will be entered directly into LRS using existing services of APIs and portal held in the ULR |
| A.03 | Must | Assumed | LARS will hold and master Pathways and Specialisms input by Ofqual |
| A.04 | Must | Assumed | ESFA will define which learning providers can offer which TQs |
| A.05 | Must | Assumed | AOs will specify which learning providers will offer TQs for which they are responsible |
| A.06 | Must | Assumed | T Levels do not store employer data nor a provider’s relationship with an employer offering industrial placements now |
| A.07 | Must | Assumed | An email notification service already exists and can be reused |
| A.08 | Must | Assumed | We will reuse EPAO printing service |
| A.09 | Must | Assumed | Not all AOs will have the capability or capacity to create APIs for pathway and specialism results |
| A.10 | Must | Assumed | In the future there will be closer integration with the other T Level streams and the design does not constrain this. |
| A.11 | Must | Assumed | The T Level service will be hosted in CIP, built on Microsoft Azure Cloud, using Platform as a Service, PaaS. |
| A12 | Must | Assumed | The system is dependent on the AOs and Learning Providers to use standard codes ie ULN, UKPRN, Pathway code, Specialism code etc |
| A13 | Must | Assumed | The explicit link between Awarding Organisations and Providers through TQs will not constrain future relationships. |

Table - Assumptions

## Constraints

| Ref. | Priority | Status | Summary statement |
| --- | --- | --- | --- |
| C.01 | Must | Assumed | Not all AOs or providers will have the capability or resources to create and maintain APIs. Results and Certification will offer a portal that can be used for bulk data transfer and individual record transfer. |
| C.02 | Must | Assumed | Results must not be visible or made available prior to results day |

Table - Constraints

## Risks

| Ref. | Description | Risk  (H/M/L) | Impact  (H/M/L) | Owner | Mitigation |
| --- | --- | --- | --- | --- | --- |
| R.01 | T Level system needs to be in production in time for learner registration at the end of October 2020 | L | H | Gary Flanagan | A series of MVPs will be delivered to enable the system to go live in incremental stages, leading up to learner registration to ensure that all preparatory work can be carried out in advance. |
| R.02 | Short time frame for the AOs to develop and test the APIs | M | M | Gary  Flanagan | A portal will be provided which will offer an alternative way in which AOs can enter data into the system as part of the MPV. |
| R.03 | Industry placements not completed before the results calculation cut off point | M | H |  | Providers incentivised to ensure that industrial placements are completed |

Table - Risks

# Physical Design

## Simplified Physical Design



## Detailed Physical Design with Individual Components

### Physical Design Detail

The solution is based on the LRS PAAS design and reuses many of the design decisions from that platform. LRS provides similar data capture functionality for other qualifications, and the aim is to reuse the some of this design increase maintainability and consistency. Having a similar architecture makes any integration between the platforms simpler and could reduce development time. Use of LRS for storing all T-Level data was considered but disregarded as that system is not designed to handle the learner registration that T-Levels require, and it was decided that having a dedicated system to handle results calculation for T-Levels was more efficient and had less risk than expanding the scope of LRS.

The solution is a web application in Azure with a portal and API access via EAPIM. There will be an Azure SQL database to store all T-Level data, and finalised results will be replicated into LRS when calculated. Event Grid is used to trigger the event flows across the service and provide additional triggers to the serverless functions if the service scope is expanded.

The T-Levels web service consists of a primary web service the performs the main functionality for the application, handling data ingest and the portal. There are 4 ancillary serverless functions to provide print functionality, connectivity to LRS, GOV.UK Notify integration as well as handling the calculation of results.

The decision to split these functions out was taken as it provides the simplest method of maintaining the service should there be service expansion in the future. It’s expected that any changes to functionality will affect functionality provided these serverless functions, so keeping them decoupled and in an easily maintainable state was deemed the best solution.

The following are core components of the system:

* DfE Sign In – Provides access to the system both through the API and the Portal. This provides identity management, credential management, authentication and roles for users of the service.
* Portal – Decoupled from the business logic and hosted on its own externally facing app instance. UI and repeated data (provider and qualification data) caching is provided by the Redis cache. The cache minimises the calls to the T-Level database when rendering provider, AO and qualification data in the portal as this data should remain static.
* REST API through EAPIM – A REST API is provided through the Enterprise API Management Gateway following the DfE API Gateway pattern and ESFA best practise.
* The T-Levels backend service consists of the following components:
  + Primary T-Level Web Service – Handles all incoming and outgoing data from AO’s and Providers and provides the business logic for the Portal. The portal will connect to a series of internal API’s exposed by the web service. These are separate from the external API’s exposed via EAPIM in order to simplify versioning and reflect the rapid requirement changes on the portal that could arise from ongoing user research. Azure File Storage will store any incoming CSV files for processing, using the ULN as the reference when processing that data.
  + Print Serverless Function – Handles the collation of data from the T-Level Database and processes this to be transferred to the print provider via their API. This service is triggered by a scheduled call from Event Grid but can also be triggered manually should a request for a specific certificate arise. The function will create a temporary store to gather all the required information for the printers, process this into the required format for the printer and transfer this via the print provider’s API. The function will handle both ad-hoc or large-scale printing requests.
  + Result Serverless Function – Processes all results and stores the processed results in the database. Triggered on a schedule from Event Grid.
  + Notification Serverless Function– Generates the notifications to be sent to GOV.UK Notify. These are generated based off periodic Event Grid triggers to check if data is missing for learners.
  + Record Serverless Function – Writes results to LRS and pulls learner records into the T-Level system for data collation during printing. Triggered from Event Grid when a result is calculated, or when learner details are requested for printing.
* Event Grid – Triggers the serverless functions to perform actions based off schedules or data requirements. Also calls the Notify and Print API’s. As the service is highly event driven, it provides the key event broker functionality between the web application and the serverless functions. It also provides a simple method of integrating further event triggers in future if those requirements arise, rather than re-engineering the services. Events can be triggered by sending Custom Event Topics into Event Grid, giving control over when actions take place in the service.
* Data Storage is provided by a geo-redundant Azure SQL database with periodic backups to Azure Blob Storage. Azure Cosmos DB was evaluated but the preferred approach was to adopt Azure SQL in line with LRS for consistency.

## Reusable Components





### Reusability

The system is designed to reuse as many components as possible in order to make the best use of resources at DfE and prevent duplication. The following are either reused or are DfE common components:

* EAPIM – The system is making use of the Enterprise API Management platform to maximise visibility across DfE of the API’s and provide a common API gateway into the T-Levels application.
* GOV.UK Notify – Notify is a GDS common component that we can utilise for communication to users outside the service. We expecting to primarily make use of the email functionality provided by this component, and it means we do not have to procure our own.
* DfE Sign In – This provides the service with role-based authentication so that users can access the Portal and the API securely, without the project having to build or procure a custom IDaM solution.
* LRS – LRS will be used to store the overall T-Level results in line with other qualifications.

## Resources

The following table lists the compute resources in the above diagram and details the location, size and scaling units supported.

The primary location for all T-Level resources will be Western Europe.

Note that in general it tends to be more cost effective to opt for reduced compute units but with increased number of instances (scale out with smaller ‘machines’ rather than scaling up). However, should the system appear to be under resource stress, this can be reviewed, and the compute instances scaled up if required – this would imply an operations cost impact.

TCO over 5 years estimated at ~£150,000 based on the resource below and access to EAPIM.

|  |  |  |
| --- | --- | --- |
| **Resource** | **Attributes** | **Location** |
| App Service Plan [External] | Pricing Tier: Standard  Instance: S1  Autoscale: up to 10 instances | Western Europe |
| App Service Plan [Internal] | Pricing Tier: Standard  Instance: S1  Autoscale: up to 10 instances | Western Europe |
| Event Grid | Pricing Tier: Standard | Western Europe |
| SQL Managed Instance | Pricing Tier: General Purpose  Generation: Gen 5  Instance: 4vCore | Western Europe |

Table - Resources

## Hosting

The T Level service will be hosted on the DfE Common Infrastructure Platform (CIP) which is a Microsoft Azure Platform as a Service Cloud, (PaaS). Four environments will be provisioned:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Environment | Promotion | Scaling | Security | Sovereignty |
| Production | From pre- production | Full size | DfE Sign in  OpenId Connect  Azure Active Directory (Azure B2B) | CIP  Western Europe |
| Pre-production | From test | Full size | Standard security model | CIP  Western Europe |
| Test | From development | Half size | Standard security model | CIP  Western Europe |
| Development |  | Smallest possible | Standard security model | CIP  Western Europe |

Table - Hosting

## API design

The T-Levels system will be heavily reliant on retrieving data from master data sources, using RESTful APIs. This data will only be pulled in as and when required.

The system will utilise the DfE API strategy, using the data layer API Gateway pattern. A façade will not be required as the T-Level results and certification system will not be calling multiple backend services.

The T-Level results and certification system publish its APIs through the EAPIM. The EAPIM will log and correlate the API calls

Authentication and Authorisation will be handled through common Enterprise IDAMS providers. The system will use

* JWT
* OpenId







### API List

|  |  |  |  |
| --- | --- | --- | --- |
| **API Name** | **Format** | **Description** | **Notes** |
| Results | REST/JSON | Used by AO’s and Providers to transfer all results data into the system. Type of result will be specified in the payload. |  |
| Provider | REST/JSON | Used by AO’s to update provider information and map TQ’s to providers. |  |
| Learner | REST/JSON | Used to onboard learners and map them to pathways and specialisms. |  |
| Appeal | REST/JSON | Set a flag to alert the system that a result in the system will need updating from the AO. | Policy to define full functionality. Might be renamed PostResult. |
| Qualification | REST/JSON | Add and update TQ’s, Pathways and Specialisms. Added manually to DB in MVP.  Not MVP. | Not for this version. Will develop when service expands beyond 2021. |

GOV.UK Notify will be used to send email reminders to Awarding Organisations detailing missing assessments and to Providers detailing missing attainments for learners that need to be entered prior to the T Level calculation. This will be handled through messages provided by Event Grid.

UKRLP and LRS integration will use API’s provided by those service to transfer data.

### Data Transfers

The table below lists the data transfers between T Levels, internal systems and external systems that have currently been identified.

| **From** | **To** | **Description** | **Method** | **Entity Exposed** | **Data Items** |
| --- | --- | --- | --- | --- | --- |
| Awarding Organisations | T Level R&C | Assessment result | Result API | Learner Record | * ULN * Regulated Qualification code * Result |
| Awarding Organisations | T Level R&C | Setup Technical Qualification (Not MVP) | Qualification API | * T-Level * Route * Pathway * MAR | * Route * Pathway Regulated Qualification code * Specialism Regulated Qualification code * MAR Id |
| Awarding organisations | UKLRP | Register a provider as a TQ provider  Dependent on UKRRL | Handled outside of the service. | * TQ Provider * Route | * RN Number * UKPRN * Route Id * Route Id |
| Awarding organisations | T Level | Onboard provider | Provider API | * Route * Pathway * Specialism | * RN Number * UKPRN * Route Id * Pathway Regulated Qualification code * Specialism Regulated Qualification code |
| Awarding organisations | T Level | Onboard learner | Learner API | * Learner * Pathway * Specialism | * ULN * UKPRN * Route Id * Pathway Regulated Qualification code * Pathway assessment data |
| Awarding organisations | T Level | Create pathway appeal | Appeal API | * Appeal * Pathway | * ULN * Regulated Qualification code |
| Awarding organisations | T Level | Update pathway appeal | Appeal API | * Appeal * Pathway | * ULN * Regulated Qualification code * Appeal result |
| Awarding organisations | T Level | Create specialism appeal | Appeal API | * Appeal * Specialism | * ULN * Regulated Qualification code |
| Awarding organisations | T Level | Update specialism appeal | Appeal API | * Appeal * Specialism | * ULN * Regulated Qualification code * Appeal result |
| Provider | T-Level | MAR Result | Result API | MAR attainment | * ULN * MAR Id * Result |
| Provider | T-Level | Industrial placement | Result API | IP Attainment | * ULN * IP Id * Result |
| Provider | T-Level | Maths equivalent | Result API | Maths Attainment | * ULN * Result |
| Provider | T-Level | English equivalent | Result API | English Attainment | * ULN * Result |
| LRS | T-Level | Learner data for printing | LRS SOAP API | Learner Record | * ULN * Learner Details * Result |
| T-Level | LRS | Learner results | LRS SOAP API | Results | * ULN * RQC * Result |

Table - Data Transfers

## Security



DfE Sign In provides access both to the portal and the API, and access to resources will be administered by DfE staff. Additional access to platform administration will be restricted to members of the development team and controlled via AD groups in Azure.

The T Level system shall use Identity as a Perimeter whilst offloading physical infrastructure security to Microsoft as part of the PaaS hosting strategy. Emphasis is therefore placed on ensuring strong authentication and authorisation.

**Secrets Management**

* All secrets and keys shall be managed by Azure Key Vault.
* Applications accessing secrets held in Azure Key Vault shall do so using Managed Service Identity with least privileged access enforced.
* Production environment shall implement a rotation strategy for values stored in the vault.
* All access to Azure Key Vault is monitored and logs output to log analytics.

**Identity**

* Azure AD used for managing access to resources and platform administration.
* DfE Sign-In will provide identity management for DfE corporate resources with trusted partner organisations and trusted individual users. DfE Sign-In supports OpenID Connect, from which T Levels will derive the user’s profile and the roles they belong to. From there the T-Level system will provide the user with access to the associated functionality and data.

**Isolation**

* Azure SQL Managed instance shall be hosted in its own VNet and therefore isolated from the public cloud.
* Authentication to Azure SQL shall be managed by Azure AD using Managed Service Identities.
* Applications interfacing with SQL MI shall have VNet integration enabled.

### Data Security

Data is stored in the T Level database, Azure File Storage, Azure Blob Storage and LRS. All data is encrypted with 256-bit AES encryption, and the T Level service will use the same security standards as LRS.

#### Data at Rest

The T Level Azure SQL DB (Managed Instance) shall protect data at rest using Transparent Data Encryption (TDE). It performs real-time encryption and decryption of the application databases, associated backups, and transaction log files at rest without requiring changes to the application.

Transparent data encryption encrypts the storage of an entire database by using a symmetric key (database encryption key). The database encryption key is protected by the TDE protector. The protector is an asymmetric key stored in Azure Key Vault (Bring Your Own Key).

All data held in Azure Storage shall be protected through Storage Service Encryption using 256bit AES encryption.

#### Data in Transit

Data in transit from outside and between the Azure components shall be protected using Transport Layer Security/Secure Sockets Layer (TLS/SSL), which uses symmetric cryptography based on a shared secret to encrypt communications as over the network. By default, network traffic is secured using TLS 1.2

Azure SQL DB shall utilise Always Encrypted, ensures that any sensitive data managed in specified columns shall remain encrypted ‘in-use’ and ‘in-transit’ (In use refers to data loaded by SQL Server during in memory computations).

### C:\Users\skirsten\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\943AAADE.tmpThreat Model

The Microsoft threat model report highlighted several threats that are categorised based on the STRIDE model:

|  |  |  |
| --- | --- | --- |
| **Category** | **Description** | **Mitigation** |
| **Spoofing** | Involves illegally accessing and then using another user’s authentication information, such as username and password. | Identity checks for all DfE Sign In users. Minimum access based in role.  Limited access to the platform administration (all users must be granted permission through Azure AD). |
| **Tampering** | Involves the malicious modification of data. Examples include unauthorized changes made to persistent data, such as that held in a database, and the alteration of data as it flows between two computers over an open network, such as the Internet | All data is encrypted at rest and in transit.  Data is backed up and results are mirrored into LRS. Monitoring is in place on the Azure platform for unauthorised access. |
| **Repudiation** | Associated with users who deny performing an action without other parties having any way to prove otherwise—for example, a user performs an illegal operation in a system that lacks the ability to trace the prohibited operations. Non-Repudiation refers to the ability of a system to counter repudiation threats. For example, a user who purchases an item might have to sign for the item upon receipt. The vendor can then use the signed receipt as evidence that the user did receive the package | There is a degree of trust with AO’s and Providers to provide ESFA with accurate data. Security of systems external to ESFA is the responsibility of those organisations. |
| **Information Disclosure** | Involves the exposure of information to individuals who are not supposed to have access to it—for example, the ability of users to read a file that they were not granted access to, or the ability of an intruder to read data in transit between two computers | Access to data will be at the minimum level required for all users to perform their actions on the service. Registration is handled by ESFA, no users can access this system without ESFA verifying those users. |
| **Denial of Service** | Denial of service (DoS) attacks deny service to valid users—for example, by making a Web server temporarily unavailable or unusable. You must protect against certain types of DoS threats simply to improve system availability and reliability | Mitigation of DoS attacks is part of the CIP platform. The service is monitored for unusual traffic and DoS attacks. Scaling of the service or suspension of the service can be provided to mitigate these sorts of attacks. |
| **Elevation of Privilege** | An unprivileged user gains privileged access and thereby has enough access to compromise or destroy the entire system. Elevation of privilege threats include those situations in which an attacker has effectively penetrated all system defences and become part of the trusted system itself. | Users are given the minimum level of access required to perform their role. Platform administration is managed by DfE users authenticated though Azure Active Directory who are trusted to access the platform. |

Table - Threats

### Perimeter Security

The following technologies and concepts make up the security perimeter of the system:

#### Azure Application Gateway

Access to the web applications is restricted to traffic originating only from the Application gateway. This is ensured by configuring the T Level web portal to only accept inbound traffic that has an origin IP address matching that of the Application Gateway, this ensures that only trusted traffic can access the web applications.

#### Azure Web Application Firewall

It is intended to utilise Azure Web Application Firewall rather than the current Barracuda WAF – This is to bring all resources under PaaS as well as reduce TCO whilst achieving the same level of security. This design has recently been approved at TDA.

The WAF is a feature of the Azure Application Gateway that provides centralized protection of web applications from common exploits and vulnerabilities such as SQL injection attacks, cross site scripting etc.

Azure WAF provides the following benefits:

* SQL injection protection
* Cross site scripting protection
* Common Web Attacks Protection such as command injection, HTTP request smuggling, HTTP response splitting, and remote file inclusion attack
* Protection against HTTP protocol violations
* Protection against HTTP protocol anomalies such as missing host user-agent and accept headers
* Prevention against bots, crawlers, and scanners
* Detection of common application misconfigurations (that is, Apache, IIS, etc.)
* Azure DDoS Protection combined with application design best practices, provides defence against DDoS attacks, with always-on traffic monitoring, and real-time mitigation of common network-level attacks. With a PaaS architecture, platform level DDoS protection is transparent to the customer and incorporated into the platform.

The Azure Application Gateway WAF can be configured to run either in Detection (Passive Mode) or Prevention (Active Mode). ARM templates shall be used to set the Firewall Mode explicitly to **Prevention**.

#### Identity Management

The following technologies provide identity management capabilities in the CIP PaaS environment and makeup the backbone of the Identity as a Perimeter security concept.

##### DfE Sign In

DfE Sign In is an OpenID Connect identify provider developed by a digital team at DfE. This component allows registered users to authenticate to the T Level portal and API.

##### Azure Active Directory

**(Azure AD)** is Microsoft's multi-tenant cloud-based directory and identity management service. All administrative users for the solution shall be created in Azure Active Directory, including user accounts for accessing the SQL Database. All user identities shall be organised into roles (RBAC) that provide Just Enough Authorisation (JEA) to required resources appropriate to their role.

Azure Active Directory Identity Protection detects potential vulnerabilities and risky accounts and provides recommendations to enhance the security posture of the organisation’s identities, configures automated responses to detected suspicious actions related to the organisation’s identities, and investigates suspicious incidents and takes appropriate action to resolve them.

Azure Role-based Access Control (RBAC) enables precisely focused access management for Azure.

Note that the Azure Subscription access is limited to the subscription administrator, and Azure Key Vault access is restricted only to users who require key management access.

### Application Security

#### User Management

Groups of users and their roles are published to services. This user and role information is subsequently used to provide authentication and authorisation information to the T Level portal and API.

#### User Authentication

User Authentication for all end users will be provided by DfE Sign In.

Access to Azure SQL DB (Managed Instance) shall be restricted to users who are centrally managed via Azure Active Directory.

To ensure only authorised applications can access the database, applications that interface to Azure SQL DB shall use Azure Managed Identities to gain access to the databases. For this to function, the web services must have managed identity enabled and database access granted to the identity. The assigned identity should only be assigned the minimum privileges required for the application to function.

### Secrets Management

Communications between the client, DfE Sign In and Portal are encrypted via SSL utilising certificates generated from the internal certificate authority provisioned in the infrastructure.

The web application firewall (WAF) component, located on the security perimeter boundary, intercepts inbound traffic, presents the Service Communications certificate as if the firewall is the server end point, passes the traffic inbound to the actual server end point where the same SSL certificate is presented as the Service Communication certificate.

Azure Key Vault is used to secure application keys and secrets to ensure that they are not accessible by third parties. It shall also be used to handle requesting and renewing of Transport Layer Security (TLS) certificates, providing the features required for a robust certificate lifecycle management solution.

Access to Azure Key Vault is secured via Managed Identities. All applications that require access to Key Vault shall have Managed Identities enabled.

The following secrets shall be stored in the Azure Key Vault:

* MIAP Database Connection String
* QCF Database Connection String
* Client Secret for the External Web Service applications (T-Level Service)
* The Portal Redis Cache connection string.
* Storage Account Keys

Within the T Level Production environment, secrets stored within Key vault shall be subject to a rotation implementation to ensure values, such as storage account keys, have a finite lifetime.

### Monitoring

As this service is hosted on a multitenant PaaS infrastructure, it is essentially ‘open’ to the public internet, therefore monitoring, especially protective monitoring, is a key requirement for the LRS PaaS security solution.

The following Azure technologies shall be used to provide oversight of the service:

#### Azure Security Centre

Azure Security Centre provides unified security policy management and advanced threat protection along with providing insights into security alerts and vulnerabilities that require resolution. It provides the following core capabilities:

* Monitoring
* Compliance
* Alerting
* Reporting

#### Azure Monitor

Azure monitor enables core monitoring for Azure services by allowing the collection of metrics, activity logs & diagnostic logs that enable the provision of insights into system behaviour. It benefits from Machine Learning capabilities allowing for predictive analytics techniques to identify patterns that may indicate the precursor of either a malicious attack or application stress. It provides the following core capabilities:

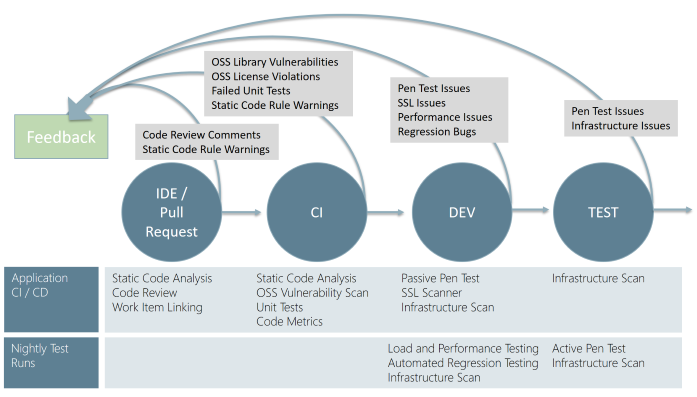
* Monitoring
* Log Analytics
* Alerts
* Reporting

Azure Monitor relies on log output generated from applications and resources. All applications shall have Application Insights enabled. Key Vault and SQL MI shall output usage data to Log Analytics for monitoring purposes.

### Continuous Validation

Key to ensuring Identity as a Perimeter is to ensure that the applications being developed do not expose unnecessary vulnerabilities or allow an attacker to exploit security loopholes that these may introduce and risk access to the data that the Identity Perimeter is there to defend.

In order to mitigate against these types of issues, the CI/CD pipelines shall introduce continuous validation – this methodology can be illustrated in the following diagram:



Pull requests/code reviews and the execution of unit tests during the CI phase will be part of the T Level SDLC.

Static code analysis that will check for vulnerabilities can be introduced into the Build Pipeline.

Dynamic vulnerability scanning (PEN testing) shall be introduced into the CD pipeline and executed as a minimum in the CI and Test environments carried out using OWASP ZAP Azure DevOps pipeline extension.

### PEN Testing Scope – Recommendations

T Level R&C PEN testing will focus on vulnerability assessments of the PaaS infrastructure as well as with the application itself.

The following table lists the resources within the PaaS solution that shall be assessed for vulnerabilities:

|  |  |  |
| --- | --- | --- |
| LRS PaaS Resource | Technology Capability | Testing Scope |
| Azure Application Gateway | * Load Balancing * Routing * Redirection (Url Rewrite) * WAF | Access to R&C is restricted to traffic originating only from the Application gateway. |
| Azure Web Application Firewall (WAF) | * Protection * Monitoring * Logging | Azure WAF protects against 10 most common OWASP Rules:   * SQL injection protection * Cross site scripting protection * Common Web Attacks Protection such as command injection, HTTP request smuggling, HTTP response splitting, and remote file inclusion attack * Protection against HTTP protocol violations * Protection against HTTP protocol anomalies such as missing host user-agent and accept headers * Prevention against bots, crawlers, and scanners * Detection of common application misconfigurations (that is, Apache, IIS, etc.)   WAF shall be configured for Prevention - Testing shall ensure the WAF is able to block above threats. |
| App Service - WebApp | * Hosting * Security | Provides the hosting service for each of the core business application components.  Testing shall ensure that the T-Level Portal and API are only accessible via the Application Gateway.  All other App Services that make up the solution are registered as Azure AD Applications and should return a 401 (Unauthorised response) when a request is issued to the public endpoint – testing shall ensure this is the case and no unauthorised requests can be made. |
| DfE Sign In | * Authentication | Testing shall ensure that unauthenticated users shall not be permitted access to the application and any session tokens cannot be intercepted for re-use. |
| Redis Cache | * Caching | Redis cache can only be accessed using a secure connection string that is stored in Azure KeyVault which only an authorised Managed Service Identity is able to retrieve.  Testing shall ensure that access to the Redis cache cannot be granted without a valid connection string. |
| Key Vault | * Authentication * Authorisation | Azure KeyVault is an AD registered resource that can only be accessed via an authorised Managed Service Identity (MSI) registered application or valid AD account.  Testing shall ensure access to keyvault is forbidden for non-authorised accounts. |
| Azure Files / Blob Storage | * Storage * Encryption * Authentication * Authorisation | Azure files & Blobs used to store data files, diagnostics and SQL backups are managed through an Azure Storage account – applications can only connect to the storage account using a secure connection string that is stored in Azure KeyVault.  Testing shall ensure that access to the Storage Account files & Blob’s is denied without possession of a valid connection string. |
| Azure SQL DB (Managed Instance) | * Authentication * Authorisation * Validation * Transactions * Logging * Monitoring * High Availability * Isolation * Encryption | Azure SQL DB (Managed Instance) underpins the solution and is responsible for storing and securing learner profiles and plans.  Testing shall ensure that access to the SQL Server instance and databases is restricted to only valid AD accounts and named user logins. Testing shall also verify that all data is encrypted at rest using TDE and any sensitive data is encrypted in transit as required. |

Table - PEN Testing Scope

## Backup, Logging and Audit

### Backup

The T-Level database application will make use of automated backups to Azure Blob Storage provided by an SQL Azure Managed Instance. Redundancy is provided across multiple Azure Data centres.

Results data is also stored on LRS, which is subject to the same backup and availability standards as the T-Level service.

### Logging and Audit

All logging and audit are performed via the tools on the CIP platform.

## Architectural / Design decisions

| Date | Decision description | Options and outcomes |
| --- | --- | --- |
| 8/10/2019 | PaaS over IaaS | PaaS has been selected as a complete development and deployment environment in the cloud |
| 8/10/2019 | Model View Controllers | Model view controllers are the standard ESFA design pattern used for developing user interfaces |
| 8/10/2019 | API.NET core | API.NET Core is an open source and can be deployed of a variety of platforms and does not restrict deployment Microsoft system software. |
| 8/10/2019 | Entity Framework Core | EF Core is an open source data access technology to provide a separation between the business layer and the database layer. It is used to send and receive data between business entities and databases. |
| 15/10/2019 | Use of RESTful APIs to transfer data from AOs | Use RESTful APIs where possible and practical to transfer information between systems to avoid rekeying and non-structured data, such as CSV files and align with industry best practice |
| 23/10/2019 | A portal will be built to augment APIs data transfer processes. | The portal will add resilience and provide an alternative for Awarding Organisations and Providers which do not have the capability or capacity to create APIs |
| 23/10/2019 | Re use of DfE Sign on component | This is a the ESFA standard |
| 23/10/2019 | Gov.uk Notify will be used for T Level email notifications | This is a the ESFA standard |
| 23/10/2019 | APIs will be published on the EAPIM | The published APIs will available for discovery and reuse when published in EAPIM |
| 23/10/2019 | The system will be built using the [standard Microsoft development toolset](#_Architectural_/_design) | This is a the ESFA standard |
| 23/10/2019 | Authentication and Authorisation will be handled through common Enterprise IDAMS providers. The system will use   * OpenId * JWT | This is a the ESFA standard |

Table - Design Decisions

## Data Persistence

Data will be persisted in the system for a minimum amount of time. Results data will be persisted in LRS for the life of the learner record. Results data will be stored in the T-Level system for 2 years based on the appeal time remaining. Printing data will be stored until receipt of the data is received by the print supplier. These limits are subject to review based on changing policy requirements.



## Document references

Where documentation already exists, provide links in the table below, or provide a summary of the scope of this document.

| Document | Link |
| --- | --- |
| Stakeholder map | https://drive.google.com/drive/folders/0AGMMiUzvxfwgUk9PVA |
| Backlog/user stories | https://drive.google.com/drive/folders/0AGMMiUzvxfwgUk9PVA |
| Sprints and iterations | https://drive.google.com/drive/folders/0AGMMiUzvxfwgUk9PVA |
| Ways of working | https://drive.google.com/drive/folders/1PGXpUfxZmx0VMX7BW0aAbmqULj6Hc2tG |

# Annexes

## Useful references

* [DfE Enterprise Architecture Principles](https://educationgovuk.sharepoint.com/sites/gp/Architecture%20Services%20Documents/DfE%20Enterprise%20Architecture%20Principles.docx)
* [DfE Business Capability Model](https://educationgovuk.sharepoint.com/sites/gp/WorkplaceDocuments/Capability/DfE%20Business%20Capability%20Model.pdf)
* [DfE architecture repository](https://educationgovuk.sharepoint.com/sites/gp/WorkplaceDocuments)
* [Example architecture diagrams](https://educationgovuk.sharepoint.com/:f:/r/sites/gp/WorkplaceDocuments/Practice/Templates/Example%20diagrams?csf=1&e=0gripF)
* [DfE IdAM strategy and patterns](https://educationgovuk.sharepoint.com/:w:/r/sites/gp/WorkplaceDocuments/Reference%20Architectures/Patterns/Pattern_IdAM.docx?d=wff10a2368c8b492897fa93d0f195b69d&csf=1&e=kNfbhH)
* [DfE technical standards](https://educationgovuk.sharepoint.com/sites/gp/WorkplaceDocuments/Standards)
* [GDS Technology Code of Practice](https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice)
* [DfE technology service offer](https://educationgovuk.sharepoint.com/how-do-i/it/Pages/service-offer.aspx)
* [Reference Non-Functional Requirement (NFRs)](https://educationgovuk.sharepoint.com/:w:/r/sites/gp/WorkplaceDocuments/Reference%20Architectures/Patterns/DFE%20Reference%20NFR's%20v4.0.docx?d=wad9f0663140a442ebd404c7837b6ce0f&csf=1&e=elBJwh)
* [Departmental Security Assurance Model (DSAM) process](https://educationgovuk.sharepoint.com/how-do-i/projects/senior-responsible-owner/Pages/information-security-risk.aspx)
* [Departmental security architecture principles](https://educationgovuk.sharepoint.com/how-do-i/it/Documents/security-policies/departmental-security-architecture-principles.docx)

## Glossary of terms

* **Application Programming Interface (API) -** a set of functions and procedures allowing the creation of applications that access the features or data of an operating system, application, or other service
* **Awarding Organisation (AO)**
* **Cloud Infrastructure Platform (CIP) -** refers to the hardware and software components -- such as servers, storage, a network and virtualization software -- that are needed to support the **computing** requirements of a **cloud computing** model.
* **Coma separated values (CSV) -** a simple file format used to store tabular data, such as a spreadsheet or database. Files in the **CSV** format can be imported to and exported from programs that store data in tables, such as Microsoft Excel
* **Department for Education (DfE) –** responsible for children's services and education, including early years, schools, higher and further education policy, apprenticeships and wider skills in England.
* **Enterprise Application Programming Interface Management (EAPIM) –** provides the ability to publish APIs with instant provisioning, automatic scaling and high availability for APIs.
* **Entity Relationship Diagram (ERD) -** a snapshot of data structures. An ERD shows entities (tables) in a database and relationships between tables within that database
* **Education and Funds Funding Agency (ESFA) -** a single agency accountable for funding education and skills for children, young people and adults
* **General Certificate of Secondary Education (GCSE) -** a set of exams taken in England, Wales, Northern Ireland and other British territories. They are usually taken by students aged 15–16, after two years of study.
* **Identity and Access Management (IDaM) -** is the combination of technical systems, policies and processes that create, define, and govern the utilization, and safeguarding of identity information, as well as managing the relationship between an entity, and the resources to which access is needed
* **Infrastructure as a Services (IaaS) -** is a form of cloud computing that provides virtualized computing resources over the internet.
* **Institute for Apprenticeships and Technical Education (Ifate) -** The Institute is responsible for the Technical Qualification (TQ). This is the main, classroom-based element of the T Level, and equips students with the skills and knowledge necessary to give them a broad understanding of their chosen occupational route.
* **Industrial Placement (IP) -** give students an opportunity to develop their practical and technical skills in a role directly relevant to their vocational course. They also give employers the chance to ensure that young people are developing the skills and experience that industry needs.
* **(LARS) –**
* **Mandatory Additional Requirement (MAR) –** additionalchecks and process to ensure that the learner has the knowledge and approval to work in their chosen pathway and specialism.
* **Oauth 2.0 (Oauth 2.0) -** the industry-standard protocol for authorisation that allows one application interacting with another on without giving away your password.
* **Office of Qualifications and Examinations Regulation (Ofqual) -** regulates qualifications, examinations and assessments in England.
* **OpenID**  an identity layer built on top of the OAuth 2.0 protocol, which allows clients to verify the identity of an end user, as well as to obtain basic profile information about the end user.
* **Platform as a Service (PaaS) -** is a complete development and deployment environment in the cloud, with resources that enable you to deliver everything from simple cloud-based apps to sophisticated, cloud-enabled enterprise applications.
* **Results and Certification System (RCS) –** provides the functionality for recording T Level assessments and supporting attainments, calculates final T Level results and prints the T Level Certificate and Certificates of Achievement.
* **RESTful API -** is an API that uses HTTP requests to GET, PUT, POST and DELETE data.
* **(RN) –** the number that is the unique identifier for an Awarding Organisation.
* **Technical Qualification (TQ) -** the technical part of a T Level, comprising of a pathway and one or more specialisms.
* **Secure File Transfer Protocol (sFTP) -** a network protocol used for secure file transfer over secure shell
* **Software as a Service (SaaS) -** a software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted.
* **UKPLR**
* **UKPRN**
* **Unique Learner Number (ULN)-** number which identifies a learner taking a T Level

**Unique Learner Record (ULR) –** a record of all the learners’ educational attainment

## Functional requirements

| Ref. | Epic | Status | Requirement |
| --- | --- | --- | --- |
| FR.01 | Must | Capture | I need the ability to confirm/suggest edits to a T-Level title |
| FR.02 | Must | Capture | I need the ability to see the approved T-Level specifications |
| FR.03 | Must | Capture | I need the ability to access a single source of all T-level data |
| FR.04 | Must | Capture | I need the ability to send ESFA T-Level specification data |
| FR.05 | Must | Capture | I need the ability to send ESFA updated specification data |
| FR.06 | Must | System access | I need to know who to contact if I can't sign-in |
| FR.07 | Must | System access | I need to know what happens if I time out of the system |
| FR.08 | Must | System access | I need to know how to sign out |
| FR.09 | Must | System access | I need to know if this is an existing account or a new account |
| FR.10 | Must | System access | I need to control portal access to some users |
| FR.11 | Must | System access | I need to know how to set up a sign-in account |
| FR.12 | Must | System access | I need to know how to retrieve lost sign-in details |
| FR.13 | Must | System access | I need to give my bespoke MI system access to the T-Level API's |
| FR.14 | Must | System access | I need to be able to find the login page |
| FR.15 | Must | System access | I need ESFA to provide me with access |
| FR.16 | Must | System access | I need to understand my levels of permissions |
| FR.17 | Must | System access | I need to provide access to approved TQ AO's only |
| FR.18 | Must | System access | I need to know how to set up a sign-in account |
| FR.19 | Must | System access | I need to know how to set up a sign-in account |
| FR.20 | Must | TQ AO's connection to T-Level | I need the ability to tell IFATE if my T-Level registration data is incorrect |
| FR.21 | Must | TQ AO's connection to T-Level | I need the ability to see which T-Levels IFATE believe I am delivering |
| FR.22 | Must | TQ AO's connection to T-Level | I need to pass TQ AO's registration data to ESFA for each T-Level |
| FR.23 | Must | TQ AO's connection to T-Level | I need the ability to check which T-Levels I am delivering |
| FR.24 | Must | Provider connection to T-Level | I need the ability to keep my T-Level details up-to-date |
| FR.25 | Must | Provider connection to T-Level | I need to maintain a register of T-Level providers |
| FR.26 | Must | Provider connection to T-Level | I need the TQ AO and providers to have I need the ability to view what they are delivering |
| FR.27 | Must | Provider connection to T-Level | I need to link a registered provider with a T-Level, it's specifications and core subjects |
| FR.28 | Must | Provider connection to T-Level | I need to change or remove a provider’s link to a T-Level, it's specification and core subjects |
| FR.29 | Must | Provider connection to T-Level | I need to upload providers and their associated T-Levels in bulk |
| FR.30 | Must | Provider connection to T-Level | I need to understand how often and from where, data is updated |
| FR.31 | Must | Provider connection to T-Level | I need to be able to remove providers |
| FR.32 | Must | Provider connection to T-Level | I need to be able to integrate MI Bespoke system with the RRC system via API |
| FR.33 | Must | Provider connection to T-Level | I need the ability to check the details I've sent about providers are correct |
| FR.34 | Must | Learner registration | I need my details recorded against the correct T-Level |
| FR.35 | Must | Learner registration | I need the ability to change registered learners’ details if they are incorrect |
| FR.36 | Must | Learner registration | I need the ability to search learner information |
| FR.37 | Must | Learner registration | I need the ability to register a learner and all of their information |
| FR.38 | Must | Learner registration | I need to be able to view the pathway and assessment date |
| FR.39 | Must | Learner registration | I need to be able to view specialism and assessment date |
| FR.40 | Must | Learner registration | I need to know the provider TQ |
| FR.41 | Must | Learner registration | I need the ability to search learners using ULN |
| FR.42 | Must | Learner registration | I need the ability to upload data in the correct format with minimal data manipulation |
| FR.43 | Must | Learner registration | I need T-Level data to be accurate |
| FR.44 | Must | Learner registration | I need the ability to search learner data from the providers |
| FR.45 | Must | Learner registration | I need the ability to register learners in bulk |
| FR.46 | Must | Learner registration | I need a single source of truth for registration data |
| FR.47 | Must | Learner registration | I need my data to be accurate and up-to-date |
| FR.48 | Must | Learner registration | I need to send my registration data to TQ AO's |
| FR.49 | Must | Learner registration | I need one data store to hold my learner data |
| FR.50 | Must | Learner registration | I need visibility of learner registration data |
| FR.51 | Must | Learner registration | I need a consistent way of identifying learners |
| FR.52 | Must | Learner registration | I need access to LRS |
| FR.53 | Must | Results | I need 3rd parties to submit accurate TQ, MAR, IP & English and Maths scores |
| FR.54 | Must | Results | I need access to LRS |
| FR.55 | Must | Results | I need to be able to retrieve the most relevant results for pathways, specialisms, maths and English, MARS and IP for technical qualifications |
| FR.56 | Must | Results | I need to provide results to UCAS, Ifate and Providers |
| FR.57 | Must | Results | I need to calculate overall scores and update the result in LRS |
| FR.58 | Must | Results | I need to tell ESFA when a learner has completed the MAR and IP |
| FR.59 | Must | Results | I need to understand which parties are willing to provide results |
| FR.60 | Must | Results | I need to supply the correct and validated data |
| FR.61 | Must | Results | I need results to be displayed in LRS |
| FR.62 | Must | Results | I need results to be submitted to LRS |
| FR.63 | Must | Results | I need to know what data I am responsible for submitting and when |
| FR.64 | Must | Results | I need to know how to validate a Learners MARs, IP & English and Maths |
| FR.65 | Must | Results | I need to remind providers that some attainments are missing |
| FR.66 | Must | Results | I need the ability to enter IP & MAR components into the results and certificates system |
| FR.67 | Must | Results | I need the ability to enter Maths & English into LRS |
| FR.68 | Must | Results | I need the ability to enter Maths & English into LRS attainments gained abroad |
| FR.69 | Must | Results | I need the assessment data for pathway and specialism results entered into LRS |
| FR.70 | Must | Results | I need to make the results available to Ifate, Providers and UCAS |
| FR.71 | Must | Results | I need to be able to calculate results instantly |
| FR.72 | Must | Results | I need to confirm equivalent Maths and English results for a learner |
| FR.73 | Must | Results | I need to know what format learners want their statement of achievement in |
| FR.74 | Must | Results | I need understand how my grade was calculated |
| FR.75 | Must | Results | I need all TQ component scores are available LRS |
| FR.76 | Must | Appeals | I need the ability to inform ESFA regarding learner appeals |
| FR.77 | Must | Appeals | I need the ability to submit new assessment scores whilst ensuring the appealed scores are also kept |
| FR.78 | Must | Appeals | I need to understand key dates and deadlines around appeals |
| FR.79 | Must | Appeals | I need to settle the appeal process before deadline |
| FR.80 | Must | Appeals | I need to ascertain if there are outstanding appeals in place for a learner and which they are |
| FR.81 | Must | Appeals | I need to provide a resolution to an appeal |
| FR.82 | Must | Appeals | I need the appeal result to be made available immediately after the decision has been made |
| FR.83 | Must | Appeals | I need the status of a learner to change when an appeal is lodged |
| FR.84 | Must | Appeals | I need to know how the appeal process works |
| FR.85 | Must | Appeals | I need recalculate the overall result based on an appeal |
| FR.86 | Must | Printing | I need to know where to send certificates and statement of achievements |
| FR.87 | Must | Printing | I need to know how to request reprints |
| FR.88 | Must | Printing | I need to present certificates to my learners |
| FR.89 | Must | Printing | I need to know how to request a statement of achievement for a learner |
| FR.90 | Must | Printing | I need it to be easy to understand my certificate |
| FR.91 | Must | Printing | I need to be able to share my certificate with employers or providers |
| FR.92 | Must | Printing | I need confirmation that the certifications and statements of achievements have been printed |
| FR.93 | Must | Printing | I need know how to send assessment data for printing |
| FR.94 | Must | Printing | I need to know when I should send certificates to print |
| FR.95 | Must | Printing | I need the ability to bulk send certificates to print |
| FR.96 | Must | Printing | I need to integrate with 3rd party printing services |
| FR.97 | Must | Printing | I need to know what to do if my job fails to reach the printer |
| FR.98 | Must | Leavers, movers and re-joiners | I need to handle changes to T-Level courses when learners come back |
| FR.99 | Must | Leavers, movers and re-joiners | I need to understand the rules around dropping out and re-joining |
| FR.100 | Must | Leavers, movers and re-joiners | I need to know which changes I need to tell my provider about |
| FR.101 | Must | Leavers, movers and re-joiners | I need to be able to request a statement of achievement if a learner drops out of a course |
| FR.102 | Must | Leavers, movers and re-joiners | I need to see the latest learner status |
| FR.103 | Must | Leavers, movers and re-joiners | I need to know when a learner status has changed |
| FR.104 | Must | Leavers, movers and re-joiners | I need to inform TQ AO's about a learner status change |
| FR.105 | Must | Leavers, movers and re-joiners | I need the ability to change a learner’s status and status date |
| FR.106 | Must | Leavers, movers and re-joiners | I need all changes to learner details to be made available in near real-time |
| FR.107 | Must | Leavers, movers and re-joiners | I need the ability to send drop-out information to ESFA |
| FR.108 | Must | Leavers, movers and re-joiners | I need the ability to send re-joiner information to ESFA |
| FR.109 | Must | Leavers, movers and re-joiners | I need to register a re-joiner on a pathway and specialism |
| FR.110 | Must | Leavers, movers and re-joiners | I need to understand which assessments a learner has undertaken in a previous T-Level will count towards a different T-Level |
| FR.111 | Must | Leavers, movers and re-joiners | I need to have up-to-date status information for learners |

## Document control

### Expiry or review date

We will review this design pack upon a significant design change.

### Version control

| Version | Date issued | Brief summary of change | Name |
| --- | --- | --- | --- |
| V0.01 | 9/10/2109 | Initial draft | Nick Fribbens |
| V0.02 | 14/10/2019 | First revision | Nick Fribbens |
| V0.03 | 17/10/2019 | Second revision | Nick Fribbens |
| V0.4 | 20/10/2019 | Including comments from peer review | Nick Fribbens |
| V0.5 | 22 /10/2019 | Including comments from peer review | Nick Fribbens |
| V0.6 | 23/10/2019 | Including comments from peer review | Nick Fribbens |
| V1.0 | 25/10/2019 | First release | Nick Fribbens |
| V1.2 | 28/11/2019 | Release for Peer Review | Sam Kirsten |

### Document approval

| Name | Role | Date |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |