**3 Compliance**

This section covers the governance of the architecture and its compliance to programme principles and standards. The approach and rational behind the approach to the delivery of the architecture is explained along with key architectural decisions, and traceability to functional and non-functional requirements.

# 3.1 Approach

The project will conform to the architectural principles laid out within the Technical Guidance Library and it is not anticipated at this stage that any deviation will be required

As a data publisher, the P&I service is not the owner of the data it receives from its sources and as such it is incumbent on those sources to ensure that any information provided is correct and where necessary additional functions (i.e. redaction) have already been performed prior to receipt. Any business rules to be applied by the P&I service (i.e. dates to publish and retention periods) will be provided by data source owners for inclusion.

However, the P&I service will be building its own meta-data content, which it will master, so that information around access and MI is captured (e.g. audit logs & usage stats).

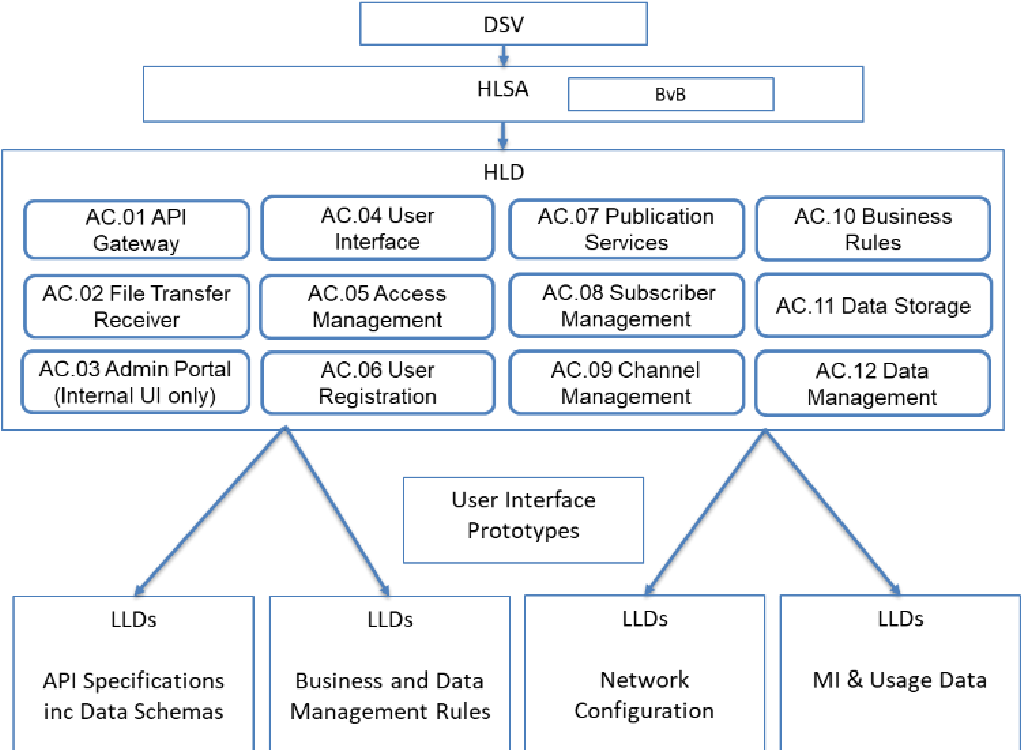
As part of a hybrid build approach existing services will be leveraged where possible. These have included:

|  |  |
| --- | --- |
| Hearings Management Interface (HMI) | Reused scripts, templates, config, set-ups and devops including networking and certificates in building the API Gateway  Logic for Gateway MI reporting  Used by S&L as a mechanism to communicate with P&I |
| Data Transfer Utility (DTS DTU) | Utilising the DTU “Lift & Shift” pattern to support file ingestion from legacy sources |
| Design Guidelines | Following HMCTS & GOV.UK standards for governing UI design |
| CRIME & CFT IDAMs | Using existing CRIME & CFT IDAMs for User Authentication (where they host relevant users) and CRIME (Common Platform Change Team) and CFT MyHMCTS user/organisation registration processes |
| GOV.NOTIFY | Utilising existing approach for registration of subscriptions and sending of emails to subscribers |
| Legacy Specifications | Analysis of existing schemas from ingestion sources and consumers (e.g. Xhibit, Libra, Crime Portal & Courtel) to help create API Schemas |
| Crime Portal | Design time concepts and templates inc. analysis of REST specifications (as above) aiding understanding of process flows, typical rules, table structures, log contents and UI layouts.  Further reuse was not applicable as a foundation for the P&I service, specifically as it was not designed to be a publication portal and would have needed significant rework and understanding of the embedded code base to remodel and rewrite which would have made it unviable |
| Strategic Data Platform (SDP) | Capturing of audit logs & reporting controls inc security events |

How these apply to specific P&I components have been presented during DSV & HLSA phases.

## 3.1.1 Documentation Approach

The P&I Service is intended to be delivered as a componentised service with contributions and collaboration from a number sources, which may be worked on in parallel. However, these will all be defined within a single HLD that will act as an overarching document. However, due to the number of moving parts, LLDs will be delivered as component level documents that can be approved separately and worked on in parallel. Existing P&I services are carried out in a number of places and by a variety of publishers and it has been agreed not to document these as part of this project.



The following table provides a guide to P&I Documentation:

|  |  |  |
| --- | --- | --- |
| **Doc Ref** | **Document Name** | **Format** |
| **PIHD001** | DSV (Digital Solution Vision) | Confluence |
| **PIHD002** | HLSA (High Level Solution Approach) | Word Document |
| **PIHD003** | BvB (Buy vs Build) | Word Document |
| **PIHD004** | HLD (High Level Design) | Word Document |
| **PIHD005** | LLD - API Specifications inc Data Schemas | Word Document & YAML |
| **PIHD006** | LLD – Business and Data Management Rules | Excel |
| **PIHD007** | User Interface Prototypes | AXURE |
| **PIHD008** | LLD – Network Configuration | Azure |
| **PIHD009** | LLD – MI & Usage Data | Word Document (SDP template) |

# 3.2 Architecture Principles

The following table explains how the project adheres to the REFORM programme architecture principles

|  |  |
| --- | --- |
| A. Be user and business centric | Will align with other Reform UIs to deliver the best UX for user groups |
| B. Understand our Data | Provide meta-data definitions to control and secure our data  Any API body and payloads will be well defined, relevant to the API call and logically structured to reflect relationships between data items. |
| C. Never compromise on Security and compliance | Publication Services and API & File Gateways will be developed and configured to make use of security standards and best practises as defined in the TGL and industry best practise. |
| E. Be Leading edge, not Bleeding edge | Making use of PAAS (Azure API Manager) and RESTful APIs which are all current technology patterns. Also, all stages of the development lifecycle are implemented on the Azure subscriptions (environments) using DevOps principles including CI/CD. |
| F. Cloud before on-premise | All components will be hosted on the Azure cloud |
| G. Be robust | The technologies selected (e.g. MS Azure API Manager), the patterns in use and the supporting technologies supporting technologies we will be using for application logging and monitoring (Dynatrace), security logging and monitoring (Log analytics workspaces/SPLUNK) will ensure that the solution built is stable and robust in design and operation. |
| H. Automate as much as possible | Data retention, user subscription and user housekeeping jobs will be fully configurable & automated Development and test processes will make use of DevOps processes and tools using CI/CD pipelines, version control and Infrastructure as Code. |
| I. Share and reuse knowledge | During design and build the project will be canvassing and sharing patterns and principles used. |
| J. Technical Guidance Library always prevails | The TGL will always be used as the 1st principle to adopt for the different areas of the design with exceptions sought where this is not possible. |
| K. Ingestion | Data sources MUST send atomic data objects that are self-contained and do not require data from other sources to fulfil their primary purpose. |
| L. Storage | All data will be stored as received - there will not be any manipulation in anyway, e.g. payloads will be held as blobs in the data store. |
| M. Presentation | Where required, presentation logic will contained in templates that will organise and format data from the data store for consumption. These will utilise HTML, CSS etc. |

# 3.3 Policies and Standards

Where possible all policies and standards will follow TGL standards as outlined below. At the current HLSA phase no requirements for deviations have been identified.

|  |  |
| --- | --- |
| Application Design | Will follow TGL guidelines:  Applications & Core Technologies  and will take account of other jurisdictions as they come on board |
| Service Design | Designed using TGL API Guidelines:  API Strategy & Vision |
| UI Design | Following design and style guidelines:  HMCTS Design System Standards  And  GOV.UK Design System Standards  And following GDS service-assessments |
| Security | Will comply with all security policies and standards that apply to HMCTS/MoJ and be compatible with HMCTS/MoJ security systems and infrastructure  Security & Compliance |
| Devops | Will follow TGL DevOps Guidelines  DevOps Guidelines |

# 3.4 Architectural Decisions

The following log explains the key architectural decisions made in the production of the architecture.

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **Date** | **Decided By** | **Decision and Rationale** |
| **AD.01** | 27/04/2021 | SDS PDG (DSV) | **The P&I Service will be a DRA Item for Publications**  The P&I Service, whilst initially, being delivered for Future Hearings, will become a reusable DRA component for Publications |
| **AD.02** | 04/05/2021 | SDS PDG (BvB) | **The P&I Service will be delivered by a Hybrid Build Approach**  As part of the Buy vs Build process a Hybrid Build Approach is to be taken to leverage existing functionality from currently deployed services (e.g.  HMI & Crime Portal) to meet Crime MVP timescales |
| **AD.03** | 27/04/2021 | SDS PDG (DSV) | **Data Ingress to the P&I Service will always be via a Gateway**  The usage of a Gateway will provide a standardised and controlled entry point to the P&I service to protect its boundary. This will include secure access, audit and throttling |
| **AD.04** | 27/04/2021 | Project | **HMI is to be used as the API Gateway for Future Hearings Information ONLY**  The HMI (Hearings Management Interface) Gateway is the strategic tool of choice within FH for API based data transfer from S&L |
| **AD.05** | 27/04/2021 | SDS PDG (DSV) | **DTU is to be used for File Based Transfers**  The DTU (DTS Data Transfer Utility) is the strategic tool of choice for File based transfer |
| **AD.06** | 27/04/2021 | Project | **Will ONLY accept API event based information in agreed standardised API schema formats**  Standardised API Schema formats will be developed in collaboration with data sources during the LLD phases. Should data received fail validation a standard API error message (400) will be returned |
| **AD.07** | 27/04/2021 | Project | **Will NOT be responsible for any transformation work or other payload manipulation (i.e. conversions of document formats from .doc to .pdf)** The rendering of information will be the responsibility of the data consumer. Only locked file formats can be accepted  P&I Service is not a master data source and does not have processes for validation and approvals, so will not update any information it receives. If an error is found by a user this should be corrected at source and resent as an update |
| **AD.08** | 27/04/2021 | Project | **The configuration of rules MUST be the responsibility of the Data Source Owner**  The P&I service is the guardian of the data it holds and so will enforce any rules applied, however, it will not set them |
| **AD.09** | 27/04/2021 | Project | **Data sensitivity & classification relating to content MUST be provided by data sources**  The P&I service must be provided with a data classification by its data sources so that it is able to apply rules to restrict access to sensitive data otherwise defaults will be applied |
| **AD.10** | 11/08/2021 | Project | **File Transfer will follow a lift and shift pattern**  As per Arch Decision (File Based Patterns) PDG v1.0 file transfer will follow the Option 1: Lift and Shift Pattern. File to API type interaction is not required |
| **AD.11** | 19/08/2021 | Project | **Business Rules will be implemented using Java Code**  This decision was reached further to the result of a design spike where the usage of Rules Engine (Drools), either as a new configuration or reused from existing Crime implementations, was considered against writing Java Code within the P&I service. |
| **AD.12** | 15/07/2021 | Project | **Business Rules and Definitions Evaluated using Decision Tree Logic** |
| **ID** | **Date** | **Decided By** | **Decision and Rationale** |
|  |  |  | After assessment of business rules requirements and their complexity it was determined that the most appropriate way for them to be defined was to use decision tree type logic |
| **AD.13** | 24/09/2021 | IWG –  Integration  Working  Group | **API Methods to follow HTTP Standards**  POST – Additive transactions (inserts a new record every-time)  PUT – Idempotent Transactions (controlled by data source either creating or overwriting an existing record) |
| **AD.14** | 21/09/2021 | Project | **Only Coarse Grained Access Control will be required for MVP**  Whilst redaction will be carried out at source it MUST be applied at the artefact header level (and not the field level). If two versions of a document, redacted & non-redacted, are required then the source system MUST send them twice with appropriate data classifications and redaction having being applied |
| **AD.15** | 30/09/2021 | Security  Architecture  () | **Usage of Verified/Un-verified Users Terminology**  Verified Users being those having been either authenticated by an IDAM  OR subscribers having had their e-mail addresses verified by Court Staff Un-verified Users being users that access the P&I service via the UI without having been authenticated |
| **AD.16** | 27/09/2021 | DWG – Data  Working  Group | **Housekeeping Service responsible for Removing Aged Artefacts and Inactive Subscriptions**  Subscriber deactivation and artefact retention is driven by a scheduled housekeeping service as opposed to business logic that could be applied when a subscription is matched or an artefact is accessed. |

# 3.5 Requirements Traceability

This section provides traceability to the functional and non-functional requirements that will be delivered by the architecture.

## 3.5.1 Functional Requirements

The following Functional Requirements are met by this architecture:

|  |  |  |  |
| --- | --- | --- | --- |
| **Ref** | **Functional Requirement** | **Category** | **Met** |
| **PIH001** | The ability to receive listing publication data and information (automated feeds) as raw or pre-formatted information. | Ingestion- Data Collection | Yes |
| **PIH002** | The ability to receive outcomes publication data and information (automated feeds) as raw or pre-formatted information. | Ingestion- Data Collection | Yes |
| **PIH003** | The ability to receive judgments publication data and information (automated feeds) as raw or pre-formatted information. | Ingestion- Data Collection | Yes |
| **PIH004** | The ability to ingest data from reform and non-reformed services (HMCTS systems) for PIH Data and Document needs. | Ingestion- Data Collection | Yes |
| **PIH005** | The ability to manually upload data as a contingency should automated publishing functionality not be available. | Ingestion- Data Collection | Yes |
| **PIH006** | The ability to update a pre-formatted publication (e.g. PDF/word) through publication of a replacement (not via changing the payload) | Ingestion- Data Create/Update | Yes |
| **PIH007** | The ability to remove a certain field through invoking an update API method. | Ingestion- Data Removal | Yes |
| **PIH008** | The ability to remove an entire document. | Ingestion- Data Removal | Yes |
| **PIH009** | The ability to receive live case status information through automated feeds as raw information. | Ingestion- Data Collection | Yes |
| **PIH011** | The ability to send publications (pre-formatted or raw) to an external archive for superseded documentation. P&I may be involved in sending Judgments to The National Archives (TNA) which can be accessed by anyone (MOJ policy project currently in progress) & lists, outcomes and judgments to SDP which is accessed by academics – which could be a mixture of raw & preformatted information. *NB: This is not a definite requirement yet – P&I will have to work with MoJ as their project (Judgments storage and publication project) progresses to see how and if P&I can be involved in sending judgments to TNA* | Data storage & Access-  Publishing Data Storage | Yes |
| **PIH012** | The ability to display data for specified periods of time as determined by the business rules. | Data storage & Access-  Publishing Data Storage | Yes |
| **PIH013** | The ability to display labels on the user interface in Welsh or English. | Data storage & Access- Publishing UI Actors | Yes |
| **PIH014** | The ability for the general public to access and view the published data on external websites without any requirement to register in the service. | Data storage & Access- Account Management | Yes |
| **PIH015** | The ability to register a user. | Data storage & Access- Account Management | Yes |
| **PIH017** | The ability to provide identification and authentication controls. | Data storage & Access- Active Directory | Yes |
| **PIH018** | The ability to manage user accounts once registered, including the ability to reset passwords. | Data storage & Access- Account Management | Yes |
| **PIH019** | The ability to provide controls to restrict access to published data. | Data storage & Access-  Data Permission  Control | Yes |
| **Ref** | **Functional Requirement** | **Category** | **Met** |
| **PIH020** | The ability to validate an existing account is active or inactive. | Data storage & Access- Account Management | Yes |
| **PIH021** | The ability to restrict the names of individuals, who are included within any publication, from appearing in search engine results. | Data storage & Access- Security Policy | Yes |
| **PIH022** | The ability to configure access rules for user groups. | Data storage & Access- Rules Engine | Yes |
| **PIH023** | The ability to display data in accordance with Data Protection and GDPR requirements. | Data storage & Access- Data Policy | Yes |
| **PIH025** | The ability to display the latest data and published documentation. | Consumption- Publishing UI | Yes |
| **PIH026** | The ability to manage published list types. (place-holder awaiting Crime workshops - warned/firmed) | Ingestion- Publishing UI | Yes |
| **PIH027** | The ability to structure the data dependant on publication type (Lists, Outcomes, Judgments templates). | Consumption- Publishing UI | Yes |
| **PIH028** | The ability to allow or restrict printing from the browser. | Consumption- Publishing UI | Yes |
| **PIH029** | The ability for a user to confirm their agreement to T&Cs before downloading or printing from P&I User Interface. | Consumption- Auditing | Yes |
| **PIH030** | The ability to display data in accordance with the GDS Style Guide service standards. | Consumption- Publishing UI | Yes |
| **PIH031** | The ability for users to **search**, filter and sort data by specified criteria (Not for pre-formatted data). | Consumption- Publishing UI | Yes |
| **PIH032** | The ability to view publications on court screens. | Consumption- Publishing UI | Yes |
| **PIH033** | The ability for Criminal Justice Partners and Third Party commercial organisations to access the published data (in line with any data agreements made with HMCTS). | Consumption-  Publishing Data | Yes |
| **PIH035** | The ability for live case status updates to be displayed via P&I online (HMCTS managed content pages which will be accessed via gov.uk). (Crown only) | Consumption-  Publishing Data | Yes |
| **PIH036** | The ability to display lists in Welsh. | Consumption-  Publishing Data | Yes |
| **PIH037** | The ability to subscribe to allow receipt to publications of interest being received via email attachment (See section 6.3.1.1 for more info on subscriptions) | Consumption- Publishing UI | Yes |
| **PIH038** | The ability to configure publication rules as defined by a set of business rules. | Data storage & Access- Rules Engine | Yes |
| **PIH039** | The ability to track manual intervention. | Data storage & Access – Auditing | Yes |
| **PIH040** | The ability to represent PDF formatted lists in the same format they are ingested | Consumption - Publishing UI | Yes |
| **PIH041** | The ability to format lists whereby the data is ingested in raw format using a template | Consumption - Publishing UI | Yes |
| **PIH042** | Will be visible on supported browsers and devices in a readable format in-line with the current GDS standards https://www.gov.uk/service-manual/technology/designing-fordifferent-browsers-and-devices | Consumption - Publishing UI | Yes |
| **PIH043** | The ability to notify users about publications of interest where there is a change or update by email | Consumption - Publishing UI | Yes |

## 3.5.2 Non-Functional Requirements

The following Non-Functional Requirements are met by this architecture.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **NFR Ref.** | **NFR Section** | **NFR SubSection** | **Categorisation** | **Requirement Description** | **Priority** |
| **ACC-01** | Accessibility | Accessibility | Requirement | All user interfaces within Reform must meet level AA of WCAG 2.1 | Mandatory |
| **ACC-03** | Accessibility | Accessibility | Requirement | The System must not return any unhandled errors when responding to an error triggered by a user or system. Error messages must be identified by the System and explained to the user/interfacing system in order to understand the cause of the error. | Mandatory |
| **ACC-05** | Accessibility | Internationalisa tion | Requirement | Solution must be able to switch between Welsh language and English language for all static content and labels. | Mandatory |
| **AUD-01** | Audit | Audit Trail | Requirement | Audit entries must be stored for 6 years, and entries must be archived and/or deleted after this time. | Must |
| **AUD-02** | Audit | Audit Trail | Requirement | Audit trail records must be held against all reference data and data associated with business critical activity. Audit records must include: - The identity of the user; System date & time;   * Identity of the host terminal/PC; * details of the transactional/event/user action; * Copies of the new and old values where data has been changed | Mandatory |
| **AUD-03** | Audit | Audit Trail | Requirement | The system must keep records of all failed, illegal and irregular events such as (but not limited to): - Failed log-ons;  - Attempts to carry out actions for which the user is not authorised | Mandatory |
| **AUD-05** | Audit | Audit Trail | Requirement | The System must ensure that all user initiated create, update and delete actions are logged for auditing purposes. These use cases would be limited to P&I system administrators via the admin portal. |  |
| **AVL-01** | Availability | Location | Requirement | The system must be accessible to office based and remote professional and HMCTS users | Mandatory |
| **AVL-07** | Availability | High Availability | Requirement | Typical failure scenarios should be identified in the detailed technical designs. The frequency and outage required for each failure scenario needs to be estimated | Mandatory |
| **SUP-10** | Supportability | Operational | Policy | Primary service hours are defined as 08:00 to 18:00. Secondary service hours are defined as 18:00 to 08:00. Service must be supported during the Primary service hours. Services must be available to end users during secondary service hours but will not be supported. | Mandatory |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **NFR Ref.** | **NFR Section** | **NFR SubSection** | **Categorisation** | **Requirement Description** | **Priority** |
| **AVL-11** | Availability | Resilience | Policy | All transactions must be recoverable in case of failure to complete. Repeated running of a transactions must not lead to duplication. | Mandatory |
| **AVL-12** | Availability | Resilience | Principle | System should be designed to avoid single point of failure | Mandatory |
| **DAT-02** | Data | Data management | Requirement | All data accepted by a system interface must be validated before being processed or permanently stored. Transactions containing invalid data must be rejected and the error reported. | Mandatory |
| **DAT-03** | Data | Data management | Requirement | All data captured through a user interface must be validated on entry and invalid entries rejected by the user interface, with an explanatory reason to the user. | Mandatory |
| **DAT-04** | Data | Data management | Requirement | The System must enforce all the maximum and minimum data lengths where defined by the data domain. | Mandatory |
| **DAT-05** | Data | Data management | Requirement | The System must ensure that data values conform to the relevant data domain. | Mandatory |
| **DAT-06** | Data | Integrity | Requirement | All transactions that fail should be either recovered to a consistent state or rolled back in their entirety, so that data entry can be resumed or repeated with the sole use of the enduser applications. | Mandatory |
| **INT-02** | Interoperability | Integration | Requirement | All date/times & timestamps should be recorded using UTC. Date/times & timestamps should be converted to local datetime at point of display where required. | Mandatory |
| **INT-03** | Interoperability | Integration | Requirement | Solution must comply with Integration strategy and standards | Mandatory |
| **MNT-02** | Maintainability | Availability | Requirement | The system must be capable of handling routine business change in a Configurable manner without falling below the applicable Service Levels. Examples of such changes are alterations or additions to Courts, Magistrates, Fees, etc. Reference data specific to the project must be clearly identified and update processes documented. | Mandatory |
| **OPR-02** | Operability | Audit Trail | Requirement | Audit records must be available for online analysis for at least 90 days up to any legal requirements specified within the Business Requirements. | Mandatory |
| **OPR-03** | Operability | Audit Trail | Requirement | In order to facilitate the analysis of transactions that affect several components, the System must provide a single location and format for the recording of audit information, across all System components. Generic reporting facilities shall be available for the analysis of audit information. | Mandatory |
| **OPR-04** | Operability | Audit Logs | Requirement | The following metrics must be gathered daily and made available to support staff via a daily metrics report:   * Daily business transaction counts by type * Daily counts of items transferred over each system interface * Daily counts of exceptions raised, by origin, type and severity | Mandatory |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **NFR Ref.** | **NFR Section** | **NFR SubSection** | **Categorisation** | **Requirement Description** | **Priority** |
| **OPR-06** | Operability |  | Requirement | The System must make provision for reference data updates appropriate to that system, such as telephone prefix changes, Post Office Postcode changes or the like. | High |
| **OPR-08** | Operability |  | Requirement | Appropriate date-based processing must include consideration of Leap Years, Bank Holidays, Short and Long days in all the region(s) covered by the System. | Mandatory |
| **PER-02** | Performance | Response time | Requirement | System response times must be evaluated at maximum load, with a fully populated database and shall exclude the impact of network latency.  In the assessment of response time, an operation must be timed from the moment the operation commences to when the operation is fully completed.  Where a single user operation involves a number of System operations (e.g. invoking other service operations in a sequence), the response time must be assessed for the user operation as whole, not just for each System operation | Mandatory |
| **PER-03** | Performance | Response time | Requirement | Trivial user operations (e.g. tabbing between screen controls) must be instantaneous (less than 0.25 seconds) | Mandatory |
| **PER-04** | Performance | Bandwidth | Requirement | Citizen and 3rd party facing services must be tested with a bandwidth restriction of 1Mbps and achieve the response time targets | High |
| **PER-05** | Performance | Monitoring |  | The system must be capable of monitoring response times for business transactions and reporting both Network Request Time (NRT) and (Software Request Time (SRT). | Mandatory |
| **PER-06** | Performance | Response time | Requirement | The System must provide a screen response for each operation of   * 90th percentile response time within 1 second * 95th percentile response time within 1.5 seconds • 99th percentile response time within 2 seconds unless specified otherwise within the Business Requirements for the system. This must be tested under realistic load conditions. | Mandatory |
| **VOL-01** | Volumetrics | Volume | Requirement | Whilst the P&I Service is a new product offering it is not anticipated to increase current publication demands or the user base requiring publication information. Therefore, the P&I Service MUST be able to support existing publication volumes.     * In total there are 70k Journalists, however, those that report on courts are limited and it is expected that on average there will be 1k unique media users a month * There are currently 35k subscriptions (e-mails via gov.notify) for daily court lists | Mandatory |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **NFR Ref.** | **NFR Section** | **NFR SubSection** | **Categorisation** | **Requirement Description** | **Priority** |
|  |  |  |  | * Daily RCJ court lists distribution: 3,859 (combination of public, stakeholders and media) * SJP media court lists: issued to approx. 250 journalists * SJP public lists (on GOV.UK): 6,784 (unique views from 1 Jan 2021 to 30 June 2021 - combination of public, stakeholders and media) * E-alerts subscribers list 31,824 (combination of stakeholders, legal professionals and media) * Courtel have 50k00 of their members belong to the ‘professional members’ category i.e. solicitors, barristers, media * There are 93k users of existing publication service, which includes members of the public and are not unique, as there will be duplication across data sets.     In total user numbers for the P&I service are expected to be less than 100k |  |
| **REL-01** | Reliability | Integration | Requirement | Transport failure should not result in loss of data/transaction | Mandatory |
| **REL-02** | Reliability | Resilience | Policy | System design should ensure that single points of failure are avoided | Mandatory |
| **REL-03** | Reliability | Capacity | Requirement | Proactive monitoring should be in place to monitor disk use to ensure sufficient disk space is made available for logging, data files, table space etc. | Mandatory |
| **SCA-01** | Scalability | Infrastructure | Requirement | The system as a whole must be scalable in all respects including total number of users and/or core business data, for example User Accounts, with only configuration changes and no change to core system code and/or product set. | Mandatory |
| **SCA-03** | Scalability | Infrastructure | Requirement | The system should be able to scale up or down horizontally in a dynamic fashion (Elastic scalability) while still adhering to performance NFRs | Mandatory |
| **SCA-04** | Scalability | Costs | Requirement | Lower environments such as development and testing must be proactively monitored to optimise cost by releasing/terminating resources not used | Mandatory |
| **SEC-01** | Security | Access Control | Requirement | Technical restrictions must be in place to make sure that users can only access those areas of functionality that they are specifically authorised to do so. | Medium |
| **SEC-02** | Security | Access Control | Requirement | Technical restrictions must be in place to make sure that systems can only access those areas of functionality that they are specifically authorised to do so. | Medium |
| **SEC-05** | Security | Access Control | Policy | The allocation and use of privileges shall be restricted and controlled. | Mandatory |
| **SEC-12** | Security | Access Control | Requirement | All Default system / vendor accounts are removed, or the passwords changed, privileges revoked and account disabled | Mandatory |
| **SEC-13** | Security | Access Control | Requirement | The system should enforce HMCTS password policy | Mandatory |
| **SEC-31** | Security | Access Control | Requirement | The default period before an inactive session times out shall be 30 minutes. | Mandatory |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **NFR Ref.** | **NFR Section** | **NFR SubSection** | **Categorisation** | **Requirement Description** | **Priority** |
| **SEC-33** | Security | Control | Requirement | All data transmission, except email, across untrusted networks are encrypted in accordance with HMG IA Standard 4(IS4). | Mandatory |
| **SEC-34** | Security | Control | Requirement | Integrity of data is maintained within the System and during data transmission. | Mandatory |
| **SEC-36** | Security | Control | Policy | The system shall comply with HMG Security Policy Framework | Mandatory |
| **SEC-37** | Security | Control | Policy | The System shall comply with the ~HMCTS Information Risk policy. | Mandatory |
| **SEC-38** | Security | Control | Policy | The system shall comply with the HMCTS Information Security policy | Mandatory |
| **SEC-39** | Security | Access Control | Policy | Direct access control to the primary servers or services via model connectivity | Mandatory |
| **SER-04** | Service  Continuity | Continuity | Requirement | The solution should identify typical failure scenarios within the System's technical design specification, with for each failure scenario: • An estimate of the likelihood of such a failure   * The state to which the System can be recovered (the recovery state) * The time taken to achieve such recovery (the recovery time) • The actions necessary to recover to that state   whilst, highlighted here a full FMEA analysis will be carried out during LLD phase | Mandatory |
| **SER-05** | Service  Continuity | Continuity | Requirement | Each component of the Service should be able to recover its hardware, database or application to the point of failure (e.g. via backups or re-do logs) with the agreed minimum loss of data | Mandatory |
| **SUP-01** | Supportability | Traceability | Requirement | In order to facilitate the analysis of transactions that affect several components, the system should be able to co-relate the audit trail (users) AND log entries (systems) to the transaction. | Mandatory |
| **SUP-03** | Supportability | Consistency | Requirement | All date/times & timestamps should be recorded using UTC. Date/times & timestamps should be converted to local datetime at point of display where required. |  |
| **SUP-06** | Supportability | Monitoring | Requirement | It must be possible to configure new reports, views and alerts as part of continuous service improvement. | Mandatory |
| **SUP-08** | Supportability | Monitoring | Requirement | It must be possible to set defined thresholds for utilisation and capacity, after which warnings will be alerted to 1st Line Support staff. | Mandatory |
| **SUP-09** | Supportability | Monitoring | Requirement | The Solution must ensure that application and error logs are shifted to a searchable database. | Mandatory |
| **SUP-10** | Supportability | Monitoring | Requirement | The Solution must ensure that logs are separated into categories but not limited to: Application Logs  Error Logs  Audit Logs | Mandatory |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **NFR Ref.** | **NFR Section** | **NFR SubSection** | **Categorisation** | **Requirement Description** | **Priority** |
| **SUP-11** | Supportability | Monitoring | Requirement | The solution must monitor resource utilisation at defined intervals and alert to utilisation in excess of defined thresholds to the 1st line support team. | Mandatory |
| **SUP-12** | Supportability | Monitoring | Requirement | The System must be able to categories the application and errors logs in below category but not limited to:   * Severe * Error * Warning * Info * Debug | Mandatory |
| **SUP-13** | Supportability | Monitoring | Requirement | The System must be configurable to alert the different level of errors to the 1st line support staff. | Mandatory |
| **SUP-14** | Supportability | Monitoring | Requirement | The System must be configurable to store different levels of application and error logs. | Mandatory |
| **SUP-15** | Supportability | Monitoring | Requirement | The System must log all errors for the purpose of dealing with support incidents. | Mandatory |
| **SUP-16** | Supportability | Monitoring | Requirement | The System must log and store performance metrics, which must be captured and stored for 6 months for the purpose of trend analysis. | Mandatory |
| **SUP-17** | Supportability | Monitoring | Requirement | The System must report the below in the error logs/reports but not limited to:  -Date / Time  -Username  -Human readable description of the error -Category (e.g. Error, Warning, Info). | Mandatory |
| **SUP-18** | Supportability | Monitoring | Requirement | The system must support remote monitoring of all critical components, such that the health of the system can be determined by support staff without manual intervention or reporting of issues by users. | Mandatory |
| **SUP-19** | Supportability | Monitoring | Requirement | All micro services must be observable, discoverable and calls between microservices traceable. | Mandatory |
| **SUP-20** | Supportability | Monitoring |  | Infrastructure performance metrics should be available in real-time and historically in oneminute increments over the last 24-hours covering at least the following key components.   * Overall CPU usage per physical server * CPU details per CPU per physical server * CPU stats per process * Overall memory usage per physical server * RAM usage per process * Swap file size | Mandatory |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **NFR Ref.** | **NFR Section** | **NFR SubSection** | **Categorisation** | **Requirement Description** | **Priority** |
|  |  |  |  | * Overall heap usage per component instance * MB of free disk space on each partition * Number of active threads * Garbage collection stats per JVM * NIC utilisation per physical server * NIC utilisation per NIC per physical server |  |
| **USE-01** | Useability |  | Requirement | When a business logic error occurs the user should receive an explanatory message indicating what they have done wrong. | Mandatory |
| **USE-02** | Useability |  | Requirement | When a system error occurs the user should receive an explanatory message indicating that there is something wrong with the system which has not been caused by them. | Mandatory |
| **USE-03** | Useability |  | Requirement | When an error occurs an indication as to what action the user should take should be given. | Mandatory |