Australian Medical Council Limited

Request for Tender: Development and Implementation of a National E-Portfolio to Support Prevocational (PGY1 and PGY2) Medical Training in Australia

Part C: IT Service Management Requirements

July 2023

CONTENTS

1 Introduction

1.1 Scope of This Document

This document sets out the Technical and IT Service Management Requirements for a National E-Portfolio for Prevocational Medical Training in Australia.

1.2 Contents of this Document

This document is set out under the following sections:

- Application Components
- Support Requirements
- Bandwidth and Utilisation and Latency
- Security Requirements
- System Maintenance Requirements
- Data Migration
- Interfaces
- Data Feeds
- Code Base and Customisations
- Data
- Auditing and Reporting
- Privacy and Security
- Operational
- Risk
- Change Management
- Disaster Recovering and Business Continuity Planning

2 Applications Components

2.1 Applications Components - Software as a Service and Managed Service

The following table sets out the details that vendors **proposing a cloud-based solution** need to provide:

Item #	Requirements	Mandatory (M) or Optional (O)
AC 2.1.1	Provide a service catalogue of cloud services.	M
AC 2.1.2	Provide a list of browsers and versions supported by the application.	M
AC 2.1.3	Provide areas in the system that may incur variable ongoing costs and the cost schedule of these items (GST-inclusive). i.e. storage, transactions, bandwidth usage etc.	M
AC 2.1.4	Provide details of all third-party components that are required for installation/implementation within Australian Medical Council. Please detail each dependency with respect to the application, version requirements and the memory and CPU requirements per user/device for these to function. i.e. Citrix, Flash, Silverlight	M

2.2 Applications Components – On Premise

The following table sets out the details that vendors **proposing an on-premise solution** need to provide:

Item #	Requirements	Mandatory (M) or Optional (O)
AC 2.2.1	Provide a list of application modules included in the solution proposed.	M
AC 2.2.2	Provide a list of application components required for the service to function (i.e. Microsoft Office, Microsoft .NET Framework, Java SDK, Windows, Crystal Reports, etc. and other third-party applications). For each component, please highlight the support license requirements, SLA's and associated support arrangements including the party responsible for each. ***Please provide an Architecture diagram supporting the response as an attachment*.**	M
AC 2.2.3	Provide details of all third-party components that are required for installation/implementation within Australian Medical Council. Please detail each dependency with respect to the application, version requirements and the memory and CPU requirements for these to function.	M

Item #	Requirements	Mandatory (M) or Optional (O)
AC 2.2.4	Provide a list of what virtualisation software can support the application.	M
AC 2.2.5	Provide details as to what monitoring and logging software is recommended/ supported by the application.	M
AC 2.2.6	If extra hardware is required or recommended, please provide specification details such as physical size, power requirements and installation recommendations, approximate costs and how it can be monitored for failure.	M

3 Support Requirements

The following table sets out the Support Requirements that the vendor must deliver:

Item #	Requirements	Mandatory (M) or Optional (O)
SUP 3.1	Detail how you will operate in an established, mature and comprehensive problem management process for the customer in accordance with ISO 20000-1 and ITIL v4 (2019)	M
SUP 3.2	State what help modules exist within the application.	M
SUP 3.3	Please provide detail of any training offered for internal Australian Medical Council technical staff to ensure appropriate 1st and 2nd level support for the service. Include costs, lead time, any location restrictions and numbers of attendees allowed.	M
SUP 3.4	State what technical support documentation is provided to assist internal support staff to diagnose issues (such as diagnostic procedures and information of error logs, common issues, etc.)	M
SUP 3.5	**Please provide a support schedule (in AEST), as an attachment to the Workbook detailing:** • Service Levels • Hours of available support • Process and channels to log a request • Help desk locations • Response times based on the severity of the issue • Support packages (e.g. Gold, Silver, Bronze) **Note:** The AMC may optionally elect to contract with the successful supplier to also provide ongoing support for the solution post-implementation.	M

4 Bandwidth Utilisation and Latency

The following table sets out the Bandwidth Utilisation and Latency Requirements that the vendor must deliver:

Item #	Requirements	Mandatory (M) or Optional (O)
BUL 4.1	Provide available / recommended options for reducing latency if required	M
BUL 4.2	Define and state the benchmark metrics for network utilisation of the most bandwidth intense functions (i.e. x number of concurrent transactions per second per user).	M

5 Security Requirements

The following table sets out the Security Requirements that the vendor must deliver:

Item #	Requirements	Mandatory (M) or Optional (O)
SEC 5.1	Provide a list of supporting integrated authentication and authorisation methods for users (such as SAML or Active Directory)	M
SEC 5.2	If a federated or Single Sign On (SSO) approach is supported, provide details on how this can be achieved. If it is not supported, please state if there are any future plans to implement it	M
SEC 5.3	If usernames and passwords are used as an authentication mechanism in the system, please provide information around managing their usage, expiry and rules around their length and character requirements	M
SEC 5.4	Does the system support role-based access (RBAC) and if so, list the pre-configured roles (if any), including service accounts.	M
SEC 5.5	If physical devices are used for authentication, please provide documentation on their requirements, specifications and known issues	M
SEC 5.6	State what access reviews are undertaken on a monthly basis with access removed for exiting employees and required changes undertaken on a timely basis.	M
SEC 5.7	Do access management policies exist to enforce the use of least privileges and cover items such as password length, password management and the use of root or administration privileges in line with agreed industry standards.	M
SEC 5.8	Are Root/Admin accounts used for ongoing management of systems?	M
SEC 5.9	Are logs available for user system or application access including log in, changes, access to confidential data etc.?	M
SEC 5.10	Australian Medical Council require that any certificates used for encryption keys are RSA 2048 bit or higher. Please state whether this requirement can be met.	M
SEC 5.11	Does the system allow data to be sent unencrypted over open networks?	M
SEC 5.12	State the maximum strength encryption available.	M
SEC 5.13	State the minimum strength encryption enforced.	M
SEC 5.14	State whether data is encrypted in the system’s database (i.e. at rest).	M

Item #	Requirements	Mandatory (M) or Optional (O)
SEC 5.15	In the event a user needs their account terminated immediately, will access to all open sessions be terminated, including mobile interfaces? Please detail your process.	M
SEC 5.16	Provide detail how stale accounts are looked for and removed.	M
SEC 5.17	Please highlight how many privileged accounts can access these systems - and the data that can be accessed. Please provide what type of authentication is required by privileged users.	M
SEC 5.18	Please state any security compliance you have in place, such as ISO 27001.	M
SEC 5.19	Please provide details on the current technical architecture including security mechanisms such as firewalls, VPNs, patching, intrusion prevention and network segregation.	M
SEC 5.20	State how your system defends itself from DOS and DDOS attacks and other threats.	M
SEC 5.21	State who has access to Australian Medical Council and other National E-Portfolio user data, both physically and virtually.	M
SEC 5.22	If you outsource any part of your infrastructure, provide details of the providers.	M
SEC 5.23	Do you allow copies of data to be held in escrow? If so, state on what basis.	M
SEC 5.24	Do you maintain all utilised versions of Software in code escrow? If so, how many versions?	M
SEC 5.25	Please state how you handle requests for access to Australian Medical Council data and other data to be stored by users of the e-portfolio, based on legislated access or for mandatory compliance reasons. Please detail where Australian Medical Council and other user data will be stored.	M
SEC 5.26	Provide details of how and when any Australian Medical Council data or other user data is deleted. If data is deleted, indicate whether it is a soft or hard deletion and whether it is or can be archived.	M
SEC 5.27	Provide a data architecture document showing whether and how Australian Medical Council and other National E-Portfolio users (e.g. Postgraduate Medical Councils, other health organisations) data storage, runtime code and physical execution environments are isolated from your	M

Item #	Requirements	Mandatory (M) or Optional (O)
	other customers. **Please provide response as an attachment to the Workbook.**	
SEC 5.28	Please provide details and frequency of certifications and/or third-party audits that are performed on your service. It is a requirement to provide a copy of all obtained certification to Australian Medical Council.	M
SEC 5.29	Are all systems and applications subject to a penetration test by an external firm on an annual (minimum) basis. Are these results shared, including remediation outcomes and timeframes.	M
SEC 5.30	Please provide details of your penetration testing regime.	M
SEC 5.31	Is the technology environment scanned for vulnerabilities on a regular basis (minimum monthly)? Please detail.	M
SEC 5.32	Are assets patched on systems in line with industry expectations based on standards such as Common Vulnerability Scoring System (CVSS 3.1) or similar.	M

6 SYSTEM MAINTENANCE REQUIREMENTS

The following table sets out the System Maintenance Requirements that the vendor must deliver:

Item #	Requirements	Mandatory (M) or Optional (O)
SM 6.1	What percentage of uptime can be guaranteed (per Part B - Detailed Requirements, a minimum of 99.9% uptime is required)	M
SM 6.2	State how scheduled and unscheduled outages are handled detailing how Australian Medical Council and other users are notified in such an event	M
SM 6.3	Provide details of how scheduled outages are managed and the times they occur	M
SM 6.4	State how the separations of duties for service provider employees are addressed, detailing how access to confidential data is limited.	M

7 DATA MIGRATION

The following table sets out the Data Migration Requirements that the vendor must deliver:

Item #	Requirements	Mandatory (M) or Optional (O)
DM 7.1	Please state what data migration approach is used highlighting timeframes the work can be performed (out of business hours, weekends, etc.) and who is responsible for each task	M
DM 7.2	Please provide any restrictions in relation to what kinds of data and time periods of historical data that can be migrated. Please provide indications of costs if such a restriction exists.	M
DM 7.3	If ongoing data imports are required, please state any notification required and the process that is performed	M
DM 7.4	In the event that the contract is terminated, what are the timeframes to return data to the Australian Medical Council or relevant data owner and how will this be facilitated.	M

8 INTERFACES

The following table sets out the Interface Requirements that the vendor must deliver:

Item #	Requirements	Mandatory (M) or Optional (O)
INT 8.1	Does the system provide a Web Service API that external/internal services can access? If so, please provide a document detailing the functions available and their usage including schemas, error handling methods etc.)	M
INT 8.2	Provide what web service standards and protocols are supported by the API (WS* standards, REST, JSON etc.)	M
INT 8.3	What security mechanisms are used by the interfaces between the vendor and Australian Medical Council? Some examples might be: • Transport layer security (TLS, https) • Message Security (WS-Security or other) • Firewall rules / white lists between both parties • Federated Security (WS-Federation, Web-SSO, OpenAuth / OpenID)	M
INT 8.4	***Please provide an architecture diagram in regards to connectivity and API documentation as an attachment to Workbook.***	M
INT 8.5	Please state what measures are in place to ensure the messages are sent in a reliable manner (Synchronous returns, message queuing etc.)	M
INT 8.6	Please state what interfaces are provided to extract analytical data to be used within Australian Medical Council's Business Intelligence function. Detail timeframes, methods and supported formats.	M
INT 8.7	Does the service provide automated event notifications? (i.e. an email response when a workflow has completed, or a web service message). If so, please detail what events and messages are supported.	M
INT 8.8	What other interfaces are required and what protocols are used? Please provide a complete list with technical specifications	O

9 DATA FEEDS

The following table sets out the Data Feed Requirements that the vendor must deliver:

Item #	Requirements	Mandatory (M) or Optional (O)
DF 9.1	For batch data feeds and extracts, SFTP is the preferred transport mechanism. Indicate whether it is available. List which file formats are supported (e.g. XML or flat with comma or piped delimiters, headers included or excluded).	M

10 Code Base and Customisations

The following table sets out the Code Base and Customisation Requirements that the vendor must deliver:

Item #	Requirements	Mandatory (M) or Optional (O)
CB 10.1	Provide details as to whether the Australian Medical Council code base and/or configuration options will be accessible by other tenants. If not, document how the architecture that ensures that code and configuration options are isolated.	M
CB 10.2	Please state how any customisations made to the system will be documented and recorded. Highlight how Australian Medical Council can have access to these records.	M
CB 10.3	Do you accept co-development scenarios, if so please describe?	O

11 DATA

The following table sets out the Data Requirements that the vendor must deliver:

Item #	Requirements	Mandatory (M) or Optional (O)
DATA 11.1	State the owner of all Australian Medical Council and other user generated transactional data in the system. Provide details on the various methods that Australian Medical Council or other relevant user can retrieve a copy of the data if required, including formats that the data can be retrieved in. Highlight any costs that are involved for each method.	M
DATA 11.2	Please provide your data isolation capability statement as an attachment, or, enter your data isolation capability statement in the provided Workbook.	M
DATA 11.3	Please state where the Australian Medical Council data store is physically located in all environments	M
DATA 11.4	Do controls exist to detect or manage sensitive data entering or leaving the organisation?	M
DATA 11.5	Please confirm the physical location of all data stored on behalf of Australian Medical Council. Does this physically reside in Australia	M
DATA 11.6	Do circumstances exist (i.e. back up or similar) where data or similar Australian Medical Council or other user or user organisation assets may be stored externally.	M
DATA 11.7	Do non-production environments contain or access production data.	M
DATA 11.8	Is data encrypted when stored and also in transit.	M
DATA 11.9	In the event that a data breach occurs, how will this be communicated to Australian Medical Council and in what time frame?	M
DATA 11.10	Does the organisation have policies and procedures in place to manage data breaches or incidents?	M
DATA 11.11	Do retention policies exist in regards to the management of Australian Medical Council or other user or user organisation data? Will data be securely destroyed on behalf of Australian Medical Council or relevant user organisation in line with agreed retention policies? **Note:** *Data retention periods (e.g. up to 7 years) are to be agreed prior to contract execution. Please share information on your proposed data retention policy here, or as an attachment to your response to this RFT.*	M

Item #	Requirements	Mandatory (M) or Optional (O)
DATA 11.12	Explain how the system complies with Record Keeping Standards including compliance with ISO 16175 part 3 covering records in business systems.	M

12 Auditing and Reporting

The following table sets out the Auditing and Reporting Requirements that the vendor must deliver:

Item #	Requirements	Mandatory (M) or Optional (O)
AUD 12.1	State the type of auditing and granularity of auditing performed. Specify what actions are audited (e.g. INSERT, UPDATE, DELETE) and what metadata is recorded with it.	M
AUD 12.2	State what data is captured within audit trails such as user information and the date and time records were changed. Provide details on how audit trails can be easily tracked by user and times the change was made. Indicate what audit reports come out of the box and what reports require design and creation.	M
AUD 12.3	Indicate which aspects of access logging can be configured on or off (e.g., action taken, system function, business object, and the like), and basic details of who can make the changes, how they are made and how to make them take effect (such as a restart).	M
AUD 12.4	Provide details of reporting to demonstrate the effectiveness of controls on a regular basis to customers. Items which may be presented include: • Performance Management (SLA's defined prior). • Items noted above under Areas of audit. • Capacity Management. • Risk Management (including any identified single points or failure, End of Life assets or critical / high vulnerabilities). • Change Management (number of effective / failed changes). • Open / resolved tickets undertaken for the period (including severity).	M
AUD 12.5	Provide details on process for annual review of service including presentation to Australian Medical Council Management of Service Performance and planned or suggested service improvements	M

13 Privacy and Security

The following table sets out the Privacy and Security Reporting Requirements that the vendor must deliver:

Item #	Requirements	Mandatory (M) or Optional (O)
PS 13.1	State what data you collect about Australian Medical Council and how is it kept private. In your response include: • What the data is used for • How long the data is retained • Whether the data is encrypted • Please provide a copy of or link to your organisation's Privacy Statement and how you are adhering to relevant Australian Privacy Legislation.	M
PS 13.2	State where geographically the data in the system is stored for all environments	M
PS 13.3	Are the shared computing services only used by parties that have comparable security requirements, risk profiles and risk appetites? If not, please explain why the proposed solution is still acceptable.	M
PS 13.4	Please identify any risks relating to Security and Privacy and state controls which address any identified risks.	M
PS 13.5	Please state how data storage is managed and associated costs if applicable.	M
PS 13.6	State whether any Australian Medical Council or data of other relevant parties (e.g. users, owners) is sent to internal or external parties other than Australian Medical Council staff and such other relevant parties (e.g. users, owners). Explain how it is sent, where it is sent and the reasons why. Also state whether data of any future user organisations will be sent to internal or external parties other than the organisation’s staff. Explain how it is sent, where it is sent and the reasons why.	M

14 Operational

The following table sets out the Operational Requirements that the vendor must deliver:

Item #	Requirements	Mandatory (M) or Optional (O)
OP 14.1	Provide documentation of your logical and physical server, database and physical storage availability and any underlying redundancy models.	M
OP 14.2	Please provide an architectural overview, including transitional states, for hardware, software and data stores.	M
OP 14.3	Provide documentation of how your system enables flexible scalability of capacity and performance.	M
OP 14.4	For hosted solutions, provide details around your backup regime including frequencies and processes.	M
OP 14.5	Please state recovery time from failure for: minimum, average, and maximum (Recovery Time Objective (RTO) based)	M
OP 14.6	Specify any analytic tools for Australian Medical Council data that are provided with the system or service	O
OP 14.7	In the event of data corruption, please state what is the maximum data loss that can be expected (Recovery Point Objective (RPO) based)	M

15 RISK

The following table sets out the Risk Requirements that the vendor must deliver:

Item #	Requirements	Mandatory (M) or Optional (O)
RISK 15.1	State whether your company has a formal Risk Management policy.	M
RISK 15.2	State how often risk is reported to Management and the Executive body.	M
RISK 15.3	State whether risk is required to be reported to any regulatory or external parties.	M
RISK 15.4	State what methodology is used to measure or evaluate risk within the organisation?	M
RISK 15.5	State whether a formal risk acceptance process exists to ensure risks are formally accepted and reviewed regularly.	M
RISK 15.6	State whether a control library exists to ensure the adequate level of controls are documented and mapped to identified risks.	M
RISK 15.7	State what level of independent audit is undertaken to assess or validate risk in the organisation.	M
RISK 15.8	Describe how risks are reported to Australian Medical Council including the management or remediation of residual risk within the organisation.	M

16 CHANGE MANAGEMENT

The following table sets out the Change Management Requirements that the vendor must deliver:

Item #	Requirements	Mandatory (M) or Optional (O)
CM 16.1	Please provide details of your Change Management process and how this would function between our organisations.	M
CM 16.2	Please provide details on the approach used for ongoing future releases including frequency of releases and expectations on Australian Medical Council.	M
CM 16.3	Please explain what flexibility exists around your release schedule to enable our planning for tests.	M
CM 16.4	Please state how much prior notice is provided to Australian Medical Council and/or other user organisations prior to a release and how release notes are distributed.	M
CM 16.5	Please state whether test plans are provided to assist with testing new releases.	M
CM 16.6	In regards to software customisations, please state what development resourcing capacity can be provided by you where custom coding exists.	M

17 Disaster Recovery and Business Continuity Planning

The following table sets out the Disaster Recovery and Business Continuity Planning requirements that the vendor must deliver:

Item #	Requirements	Mandatory (M) or Optional (O)
DR 17.1	Please provide a document detailing your Business Continuity Plan. Please provide an architecture document describing the overarching architecture including how any replication is performed, how backup and restoration is realised and what frequency it is performed. ***To be provided as attachments to Workbook*.**	M
DR 17.2	Please state what Recovery Time objective (RTO) can be met. Australian Medical Council generally expects a time of 4 hours or less.	M
DR 17.3	Please state what guarantees can be provided to ensure no data loss as the result of an outage. Please state what Recovery Point Objective (RPO) can be achieved. Australian Medical Council expects a time of 15 minutes.	M
DR 17.4	State what experience Australian Medical Council staff will receive during both a scheduled and unscheduled outage.	M
DR 17.5	State what human and technical processes and controls must be in place to recover from an outage.	M
DR 17.6	State what redundancy measures are required on the Australian Medical Council side for any dependent hardware or software for the system	M
DR 17.7	State what monitoring measures are required / recommended	M
DR 17.8	How often will DR and BCP plans be updated? How often will testing be undertaken to assess the effectiveness of plans?	M
DR 17.9	What evidence will need to be shared with Australian Medical Council in regard to outcomes for noted tests including response / recovery times and alignment to agreed objectives?	M