Harvard University

Application Architecture C

EA Design Review Checklist

New Version 2.3

Project Data

		Developed Solutions	Licensed Solution - Harvard's Cloud	Licensed Solution - Vendor Hosted	Subscription - SaaS	Notes
	Project Name					
	Sponsoring organization					
	Operating organization					
	Purpose of the project					
	User constituents					
*	**Solution Module or all**					
	Submitter					
	CTO Reviewer					
	Review Date					

General

G1	**Ownership**	Project **MUST** have a clearly defined business owner for development and operation	☐	☐	☐	☐	
G2	**Ownership**	Project **MUST** have a clearly defined Technical owner for development	☐	☐	☐	☐	
G3	**Ownership**	Project **MUST** have a clearly defined Technical owner for operations	☐	☐	☐	☐	
G4	**Vendor**	Licensed and subscribed software components **MUST** have had business qualification from the Vendor Management Office			☐	☐	
G5	**Vendor**	Externally hosted licensed and subscribed software vendors must **MUST** have provided SSAE19 SOC2 reports or equivalent	☐	☐	☐	☐	
G6	**Cost**	An estimated total cost of development **MUST** have been developed	☐	☐	☐	☐	
G7	**Cost**	An estimated total cost of operation **MUST** have been developed	☐	☐	☐	☐	
G8	**Cost**	The estimated total cost of ownership over time **MUST** have been agreed by the business owners	☐	☐	☐	☐	

Functional

F1	**Security**	The solution **MUST** protect data and functionality to the level needed by the sponsoring organization and appropriate to the operational risk profile of the solution.	☐	☐	☐	☐	
F2	**Security**	Solution data **MUST** be separated from other tenants, ideally by providing a dedicated database or dedicated schema.				☐	
F3	**Security**	The solution **MUST** integrate with Harvard's single-sign-on authentication service HarvardKey, using either CAS, SAML2, or other supported protocols.	☐	☐	☐	☐	
F4	**Security**	Mobile solutions, either stand-alone or adjuncts to larger solutions, **MUST** integrate with Harvard's single-sign-on authentication service HarvardKey, using either CAS, SAML2, or other supported protocols.	☐	☐	☐	☐	
F5	**Security**	The solution **MUST** provide role-based authorization to users of the solution, either as a feature of the applcation or through an authorization service such as Group Services, in accordance to the principle of least privilege.	☐	☐	☐	☐	
F6	**Security**	Solutions **MUST** conform to the appropriate HUIT security policies (https://policy.security.harvard.edu/security-requirements). Consult with your ISO for guidance.	☐	☐	☐	☐	
F7	**Security**	The solution **MUST** constrain the permitted network, service, and package interactions that are allowed, in accordance to the principle of least privilege (for example DDNS protection, port visibility black/white listing).	☐	☐	☐	☐	
F8	**User Experience**	Applications **MUST** meet the HUIT accessibility policy (http://accessibility.huit.harvard.edu/huit-policy).	☐	☐	☐	☐	
F9	**User Experience**	The solution **SHOULD** work with both computers and mobile devices. Web-based solutions should work with a variety of industry-standard web browsers.	☐	☐	☐	☐	

F10	User Experience	The solution **SHOULD** provide a modern user experience where the interface and workflow designs provide access to desired outcomes with the least friction. https://projects.iq.harvard.edu/harvarduxgroup/home	☐	☐	☐	☐	
F11	User Experience	The solution's ornamentation, including branding, color schemes, look-and-feel, and navigation schemes **SHOULD** conform to Harvard branding standards.	☐	☐	☐	☐	
F12	Applications	The solution's design **SHOULD** make use of shared services in order to avoid duplicating existing capabilities	☐	☐	☐	☐	
F13	Application	The solution **SHOULD** be instrumented so key aspects of the design, for example specific transactions or process durations, can be monitored with Harvard's chosen monitoring infrastructure: CloudWatch and Nagios.	☐	☐	☐	☐	
F14	Interoperation	The solution **MUST** clearly identify all service and external interactions including data sets transferred, frequency and schedules of flows, mechanisms and protocols of transfer, and API services used and offered to others	☐	☐	☐	☐	
F15	Interoperation	Applications **SHOULD** provide APIs (preferably REST) for loading & extracting data, for configuration, and for monitoring. Bonus point for providing APIs which permit application remote control like invoking business processes. APIs should be versioned, and as new versions are released adequate time must be given for conversion before older versions are retired. More bonus points if the APIs are authenticated and use a role-base authorization mechanism.	☐	☐	☐	☐	
F16	Data	The solution design **SHOULD** identify data managed by the solution that is considered 'system-of-record', data that is duplicated from other sources and offered to others as 'authoritative sources', and data that integrates with any master data management processes	☐	☐	☐	☐	
F17	Data	The solution **SHOULD** favor cloud-based persistence repositories, and tools	☐	☐	☐		
F18	Data	The solution **SHOULD** persist its data to a HUIT-supported RDBMS system like Oracle, MySQL, or Microsoft SQL Server	☐	☐	☐		
F19	Middleware	The solution **SHOULD** favor HUIT-supported middleware services such as IAM, databases, monitoring, logging, notification, and other services, instead of building these capabilities or using unsupported capabilities	☐	☐			
F20	Middleware	The solution **SHOULD** provide logging and audit information necessary to provide operational support and to meet our Price-Waterhouse-Coopers audit requirements.	☐	☐	☐	☐	
F21	Infrastructure	The solution **MUST** run on a modern industry-standard OS, one of Red Hat Enterprise Linux, Amazon Linux or Microsoft Windows. Linux is preferred.	☐	☐			
F22	Infrastructure	The solution **MUST** be designed for cloud deployment, and should take advantage of cloud features (e.g. supporting auto-scaling, load balancing across geographic locations, etc.).	☐	☐			
F23	Networking	The solution **SHOULD** be able to operate on internal networks *and* over the internet, unless security constraints exist	☐	☐	☐		
F24	Networking	The solution **SHOULD** be able to operate using IPv6	☐	☐	☐	☐	

Systemic

S1	Performance	The solution interface and processing **MUST** meet the responsiveness requirements set by the project team	☐	☐	☐	☐	
S2	Throughput	The solution **MUST** be designed to meet all data transfer throughput requirements in Harvard's environments	☐	☐	☐	☐	
S3	Scalability	The solution **MUST** be able to support the expected range of user, processing, and communications loads both initially and over time	☐	☐	☐	☐	
S4	Reliabliity	The solution **MUST** be able to remain functional using failure recovery techniques, in alignment to the project team requirements	☐	☐	☐	☐	
S5	Availability	The solution **MUST** be available to users in conformance to project team requirements. Maintenance downtimes must be scheduled and documented as part of a Service Level Agreement	☐	☐	☐	☐	
S6	Extensibility	The solution **SHOULD** provide a modular design that allows activation and deactivation of capabilities without disruption	☐	☐	☐	☐	
S7	Manageability	The solution **SHOULD** provide a design that allows maintenance to take place while users are still connected	☐	☐	☐	☐	
S8	Serviceability	The solution **SHOULD** provide the ability to fully or partially transition from full production operation to an off-line or maintenance mode	☐	☐	☐	☐	

Operations

O1	Schedules	The project team or vendor **MUST** document operational requirements, including a list and schedule of tasks Harvard operations and administrative staff are required to perform on the solution	☐	☐	☐	☐	
O2	Schedules	The operations team or vendor **MUST** publish availability / outage / maintenance schedules, including the agreed solution outage schedule	☐	☐	☐	☐	

	O3 Schedules	The operations team or vendor **MUST** document automated job schedules, including the job automation approach, and describe the jobs that are required for regular solution operation	☐	☐	☐	☐	
	O4 Schedules	The operations team or vendor **MUST** publish interoperation job schedules, including the frequency, timing, and approximate duration of system-to-system interactions	☐	☐	☐	☐	
	O5 Schedules	The operations team or vendor **MUST** document backup schedules, including the frequency and timing of incremental and full backups, and the retention intervals	☐	☐	☐	☐	
*	O6 Recovery	The project team or vendor **MUST** document DR & BC approaches, as well as synchronization and test schedules, including the DR and BC plan resources and testing schedules	☐	☐	☐	☐	
*	O7 Recovery	The supprt organizations **MUST** be aware of recovery procedures, runbooks, and contact information to execute available recovery processes in the event of a serious outage.	☐	☐	☐		
	O8 Support	The supprt organizations **MUST** be aware of the level 0 and level 1 support requirement from users of this solution, and intend to meet them	☐	☐	☐	☐	

Development

	D1 Environments	All projects **MUST** deploy two environments dedicated to Production and Test. Additional environments may be deployed in support of development, integration, diagnosis, staging, and other roles.	☐	☐	☐	☐	
	D2 Documentation	Technical, operational, and user documentation **MUST** be provided and should include complete technical detail such as functional and procedural guides, techncal configurations and customizations, on frameworks, libraries and services in use, on TCP/IP ports in use, etc.	☐	☐	☐		
	D3 Tools	Project team or vendor **MUST** provide tools for moving data, configurations, and other artifacts between the environments	☐	☐	☐	☐	
	D4 Tools	The project team **MUST** use a common artifact repository and version control techniques for change management	☐				
*	D5 Transition	The project team **MUST** conduct readiness tests prior to entering production, or periodically for 'Continuous Delivery' environments. These include: functional, security, accessibility and DR. Optional tests include: volume, stress, rollback, and others.	☐	☐	☐		
	D6 Tools	The project team or vendor **SHOULD** use a consistent change management toolset for code promotions, data replication, data didentification, and other cross-environment activities	☐	☐	☐	☐	
	D7 Tools	The project team or vendor **SHOULD** use a consisent set of testing tools, and processes including test plans, test cases, result, data, automation, and regression tools	☐	☐	☐	☐	

Governance

	G1 Organization	The project team **MUST** have a defined structure, generally described by an organizational chart, which describes the project team role structure and staffing	☐				
	G2 Methodology	The project team **MUST** adopt a consistent methodology to structure work and measure progress	☐				
	G3 Methodology	The project team **MUST** have documented workflows which describe design, development, testing, change management, and other processes	☐			☐	
	G4 Communication	The project team or vendor **MUST** have a reporting process that communicates status and progress to internal and external communities	☐	☐	☐	☐	
	G5 Communication	The vendor **SHOULD** be able to provide a product roadmap, and when significant change appears in that roadmap both the business and HUIT should evaluate potential impact.		☐	☐	☐	