

Government
Information
Technology
Agency

Statewide
STANDARD
P730-S730 Rev 3.0

TITLE: Applications and Related Software

Effective Date: October 31, 2007

1. AUTHORITY

The Government Information Technology Agency (GITA) shall develop, implement and maintain a coordinated statewide plan for information technology (IT) (A.R.S. § 41-3504(A (1))), including the formulation of policies to effectuate the purposes of the agency (A.R.S § 41-3504(A (13))) and adopting statewide technical, coordination, and security standards (A.R.S. § 41-3504(A (1(a))))).

2. PURPOSE

The purpose of this standard is to provide guidance and direction for budget unit and State implementations of software applications that automate business processes.

3. SCOPE

This applies to all budget units. A budget unit is defined as a department, commission, board, institution or other agency of the state receiving, expending or disbursing state funds or incurring obligations of the state including the Arizona Board of Regents but excluding the universities under the jurisdiction of the Arizona Board of Regents, the community college districts and the legislative or judicial branches. A.R.S. § 41-3501(2).

The Budget Unit Chief Executive Officer (CEO), working in conjunction with the Budget Unit Chief Information Officer (CIO), shall be responsible for ensuring the effective implementation of Statewide Information Technology policies, standards, and procedures (PSPs) within each Agency.

4. STANDARD

The following software application standards provide for more effective sharing of resources and information among budget units as well as interoperability with other governmental entities and the private business sector. Standards are also intended to encourage further deployment of systems enabling new business opportunities and providing new e-government solutions for delivering service.

4.1. **APPROACH:** Selection or development of software applications shall focus primarily on desired functionality and adaptability, driven by business requirements and rules. A foundation for interoperability and the sharing of information and resources is accomplished by aligning software applications with *Statewide Policy P100, Information Technology* which requires that budget units develop, acquire, or implement software applications and applications-related software that support open architecture, interoperability, portability, and scalability.

4.2. **SOFTWARE APPLICATIONS:** Software applications shall, where applicable, emphasize end user (State employee, community of interest, public customer) productivity and performance enhancements and enablers (decision-making at

the appropriate level) through self-service and self-administration. The underlying structure of the software applications may be n-tier or traditional, monolithic with browser (preferred) or GUI-based client access.

4.3. **INTEROPERABILITY**: Software applications shall have the capability to securely exchange information and integrate or interoperate with other applicable or related software applications.

4.3.1. Software applications shall be deployed with the following:

- Platform independence or, at a minimum, pervasive, industry-wide, commonly used platforms, to facilitate integration and interoperability.
- Non-proprietary technologies, wherever possible, to facilitate integration and interoperability.
- Open and/or de-facto standard protocols and middleware technologies, without proprietary issues, requirements, custom programming, and intermediate interface-specific applications, wherever possible, to provide consistent methodologies and techniques to accomplish the sharing of information and to facilitate inter-application communications.
- Common, proven, pervasive, and open software products (programming, database, and productivity software) to provide a consistent framework to enable integration, communication, and interoperability.
- Open programming languages (C++, Java, Visual Basic, HTML, XHTML, XML, AJAX, BPEL, WSDL etc.), wherever possible, to provide consistent structure and format.
- Open database connectivity and database middleware that use open database connectivity (SQL, ODBC, OLE DB, NDMP, NFS, CIFS, JDBC, XQuery, ESB etc.), wherever possible, to provide proven, pervasive technologies to share and exchange information.

4.3.2. **N-TIER-ORIENTED SOFTWARE APPLICATION**

ARCHITECTURE: shall be utilized, wherever possible, to facilitate platform independence and portability while offering the greatest potential for reuse and sharing of programming code.

- Software applications shall use industry- or de facto standard application programming interfaces (APIs) such as Open API, OLE DB etc., to insulate applications from the effects of platform, network, and database changes.
- Software applications shall use specifications such as CORBA, COM, DCOM, and ORB to provide for creating, distributing, and managing program objects and components in a networked environment.
- Software applications shall assemble and integrate existing, common components, where practical, rather than creating custom

code for software applications, to promote reuse and sharing of programming code.

4.3.3. Software applications should maximize the principles, recommended standards, and best practices delineated in the Target Network and Platform Architectures to provide widespread choice and flexibility for target database productivity, programming software, including middleware.

- Software applications should utilize target platform and network operating systems to allow for common, open-standards-based, management tools that are deployable across the State of Arizona Target Enterprise Architecture domains and their extension to management of applications.
- Software applications should utilize target platform and network operating systems deployed with consistency of version and most current production release to increase interoperability and portability of software applications, programming, database, and utility software, and to reduce installation, support, and maintenance costs.

4.4. **SECURITY:** Software applications shall adhere to *Statewide Policy P800, IT Security* and applicable Statewide IT security standards to safeguard the State's information and resources and establish a more trusted environment for the citizens. In accordance with *Statewide Standard P800-S805, Risk Management*, budget units shall perform a risk assessment to determine security vulnerabilities and identify specific security concerns that must be addressed before development and deployment of the software application.

4.4.1. Security services associated with software applications, databases, and utility software shall adhere to Statewide IT security standards, and

- Allow for the security controls for applications, platform, and network levels to be integrated to reduce or eliminate redundancies. Application level security shall take full advantage of network and platform security and be designed for open standards where possible to eliminate proprietary security solutions.
- Adhere to network connectivity, access, authentication, and authorization techniques as defined by Statewide IT security standards.
- Allow for all security updates to be pushed to, or accepted by, all associated software products.
- Allow for an integrated lightweight directory access protocol (LDAP) directory service.

4.5. **PATCH MANAGEMENT:** *Statewide Standard P710-S710, Network Infrastructure, Statewide Standard P720-S720, Platform Infrastructure, and Statewide Standard P730-S731, Software Productivity Tools* delineate

requirements for developing and implementing written procedures that identify roles and responsibilities for implementing patch management. Budget units shall coordinate and assess the impact of patches on software applications prior to installing the patch. Where practical and feasible, budget units shall test patches in a test environment prior to installing the patch. Testing exposes detrimental impacts to internal/external enterprise-wide application software systems, community-of-interest application software systems, and other third-party application software systems.

- 4.6. **INTELLECTUAL PROPERTY:** All software shall conform to requirements in *Statewide Policy P252, Intellectual Property* to fully comply with all legal provisions governing copyright laws and authorial integrity.
- 4.7. **CONFIGURATION MANAGEMENT:** Software applications (assets) shall be controlled, inventoried and managed in accordance with *P800-S815, Configuration Management*.
- 4.8. **TARGET SOFTWARE APPLICATION ASSESSMENT:** Given the dynamic nature of target software lifecycles and advances in the information technology industry, changes to the Arizona Target Software Application table are inevitable.
 - When a budget unit plans to implement an application not included on the current Arizona Target Software Application table¹, or programming/database software not included on the current Arizona Target Programming, Database, and Productivity Software table², the CIO shall submit a Target Software Application Architecture Assessment (Attachment A) to GITA, either in advance of or concurrent with the PIJ.
 - Initial ratings of software applications shall come from the CIO of the budget unit responsible for the application.
 - Changes to software application, programming software, or database software ratings shall come from the budget unit CIO responsible via submittal to GITA of a completed Target Software Application Architecture Assessment (Attachment A) for the application requiring change.
 - Arizona's State CIO in conjunction with the CIO Council shall have final approval of all software assessment ratings, whether conducted virtually or at a CIO Council meeting.

5. DEFINITIONS AND ABBREVIATIONS

- 5.1. Refer to the PSP Glossary of Terms located on the GITA website at http://www.azgita.gov/policies_standards for definitions and abbreviations.

¹ The Arizona *Target Software Application* table is available at http://www.azgita.gov/enterprise_architecture/NEW/Software_Arch/AppendixB.pdf

² The Arizona *Target Software Programming, Database, and Productivity Software* table is available at: http://www.azgita.gov/enterprise_architecture/NEW/Software_Arch/appendix%20C.pdf

6. REFERENCES

- 6.1. A. R. S. § 41-621 et seq., “Purchase of Insurance; coverage; limitations, exclusions; definitions.”
- 6.2. A. R. S. § 41-1335 ((A (6 & 7))), “State Agency Information.”
- 6.3. A. R. S. § 41-1339 (A), “Depository of State Archives.”
- 6.4. A. R. S. § 41-1461, “Definitions.”
- 6.5. A. R. S. § 41-1463, “Discrimination; unlawful practices; definition.”
- 6.6. A. R. S. § 41-1492 et seq., “Prohibition of Discrimination by Public Entities.”
- 6.7. A. R. S. § 41-2501 et seq., “Arizona Procurement Codes, Applicability.”
- 6.8. A. R. S. § 41-3501, “Definitions.”
- 6.9. A. R. S. § 41-3504, “Powers and Duties of the Agency.”
- 6.10. A. R. S. § 41-3521, “Information Technology Authorization Committee; members; terms; duties; compensation; definition.”
- 6.11. A. R. S. § 44-7041, “Governmental Electronic Records.”
- 6.12. Arizona Administrative Code, Title 2, Chapter 7, “Department of Administration Finance Division, Purchasing Office.”
- 6.13. Arizona Administrative Code, Title 2, Chapter 10, “Department of Administration Risk Management Section.”
- 6.14. Arizona Administrative Code, Title 2, Chapter 18, “Government Information Technology Agency.”
- 6.15. State of Arizona Target Network Architecture
- 6.16. State of Arizona Target Platform Architecture
- 6.17. State of Arizona Target Security Architecture.
- 6.18. State of Arizona Target Software Architecture.
- 6.19. Statewide Policy P100, Information Technology.
- 6.20. Statewide Policy P252, Intellectual Property.
- 6.21. Statewide Policy P700, Enterprise Architecture.
- 6.22. Statewide Policy P710, Network Architecture.
 - 6.22.1. Statewide Standard P710-S710, Network Infrastructure.
- 6.23. Statewide Policy P720, Platform Architecture.
 - 6.23.1. Statewide Standard P720-S720, Platform Infrastructure.
- 6.24. Statewide Policy P730, Software Architecture.
 - 6.24.1. Statewide Standard P730-S731, Software Productivity Tools.
- 6.25. Statewide Policy P800, IT Security.
 - 6.25.1. P800-S815, Configuration Management.

7. ATTACHMENTS

Attachment A – “Target Software Architecture Assessment”

ATTACHMENT A. TARGET SOFTWARE ARCHITECTURE ASSESSMENT

This assessment is an evaluative tool intended to determine the “readiness” level of interoperability, functionality, scalability, and adaptability of software relative to enabling new business opportunities and providing new e-government solutions for delivering service in the future. It is designed to support the planning and implementation of Target Software Architecture principles, recommended standards, and best practices. It addresses the alignment of the software applications and associated programming, database, productivity, and utility software proposed in a PIJ with Enterprise Architecture. It describes major attributes and characteristics derived from *Statewide Policy P100, Information Technology* and the principles and recommended standards and best practices contained in the Target Software Architecture.

Ratings for programming, database, and productivity software are based on the latest production release of the software. Utility software products used in conjunction with target network and platform architectures are considered target.

This assessment is applicable for all software reported to the Information Services Inventory System (ISIS) as defined by *Statewide Standards P800-S815 Configuration Management*.

Score. Questions for the four (4) software categories are scored with one (1) point for a “Yes” answer and zero (0) for a “No” answer. **Maximum possible** is the total number of questions for each category.

Agency/Community of Interest: _____

Software Application Name: _____

| Attributes/Characteristics | Maximum Possible | Score | Description |
|-----------------------------------------------------------------------------------------------------------------------|------------------|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Functionality, scalability, and adaptability, emphasizing client interaction (Software Applications only) | 5 | | Software Applications designed to fulfill business requirements and maximize the efficiency and effectiveness of business functions: able to scale and adapt as business requirements change and expand; that are interoperable, modular, and deployable across the State enterprise; and that support e-government and client self-sufficiency through browser-based access, regardless of location. |
| 2. Platform independence and use of non-proprietary technologies | 5 | | Addresses interoperability, portability, and integration across platforms utilizing open and/or de-facto standard protocols, programming languages, middleware, development tools, databases, utilities, etc. |
| 3. Exchange of information, integration with other software | 5 | | Utilizes common, standard interfaces and/or middleware having the ability to interoperate and integrate with other software without requiring custom programming or intermediate, interface-specific applications. |
| 4. Ability to maximize (take full advantage of) Target Network, Security, and Platform Architectures | 5 | | Has the capability to conform to, and adhere to, the standards and best practices delineated in the other domain architectures without requiring substantial modifications. |
| Total Rating Points | 20/15 | | |

Software when *italicized* in an assessment question encompasses all five (5) categories of Software Architecture, including:

1. Software Applications
2. Programming Software
3. Productivity Software
4. Database Software
5. Utility Software

Software Application Name: _____

| | |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| 1. Functionality, scalability, and adaptability refer to software applications that have the ability to scale and adapt as business requirements change and expand; are interoperable, modular, and deployable across the State enterprise; and that emphasize e-government and client self-sufficiency through browser-based access, regardless of location. (Software Applications only) | Yes |
| 1. Is the software application extensible (capable of being expanded or customized), adaptive (the adjustment or modification that makes something more fit given the conditions of its environment), and capable of accommodating increased demands for service without substantial modifications and additional costs? | |
| 2. Is the software application developed and deployed utilizing open and/or de-facto standard protocols, languages, development tools, databases, etc.? | |
| 3. Is a browser or GUI presentation layer available for the software application? | |
| 4. Does the software application emulate the "look and feel" of the client device's operating system and productivity software? | |
| 5. Does the software application support e-government solutions and/or end user self-sufficiency or self-service? | |
| 2. Platform independence and use of non-proprietary technologies addresses interoperability and portability across platforms utilizing open and/or de-facto standard protocols, programming languages, middleware, development tools, databases, utilities, etc. | |
| 1. Is the <i>software</i> , as configured, portable, and accessible across platforms in use within the subject agencies or community of interest? | |
| 2. Is the <i>software</i> , including version levels, consistent with current deployments of like or similar <i>software</i> within the subject agencies or community of interest? | |
| 3. Is the <i>software</i> , as configured, platform independent, without proprietary issues and requirements? | |
| 4. Is the <i>software</i> designed for, and/or supports, n-tier-oriented architecture deployment and implementation? | |
| 5. Does the <i>software</i> allow for, or provide open and/or de-facto standard interfaces for, a variety of end-user client devices, server and storage platforms, and database products? | |
| 3. Exchange of information, integration with other software emphasizes common standard interfaces and/or middleware having the ability to interoperate and integrate with other software without requiring custom programming and intermediate interface-specific applications. | |
| 1. Does the <i>software</i> , as configured, provide for and/or support (directly or through extensions) the transparent transfer and exchange of information with other software products through open or de-facto industry standards? | |
| 2. Does the <i>software</i> utilize target middleware technologies or open or de-facto industry standards for communicating and exchanging information with other software products? | |
| 3. Does the <i>software</i> provide for and/or support the integration of, or interfacing with, productivity software currently deployed within the subject agencies or community of interest? | |
| 4. Does the <i>software</i> provide the capability for sharing common software services and potential reuse of components? | |
| 5. Is the <i>software</i> , as configured, unrestricted by any proprietary or vendor-specific integration requirements? | |
| 4. Ability to maximize Target Network, Security, and Platform Architectures addresses the capability to conform to, and adhere to, the standards and best practices delineated in the other domain architectures, without requiring substantial modifications. | |
| 1. Is the <i>software</i> capable of providing and/or supporting secure (as defined by the AZ EA Target Security Architecture) end-user interface access without substantial modifications, regardless of end-user location? | |
| 2. Does the <i>software</i> , as configured, utilize target Network and Platform operating systems? | |
| 3. Are the versions of the target Network and Platform operating systems utilized by the <i>software</i> consistent with current deployments within the subject agencies or community of interest? | |
| 4. Do the security services included with the <i>software</i> align with Target Security Architecture and adhere with all security, confidentiality, and privacy policies as well as applicable statutes? If no security services are included, is the <i>software</i> unrestricted to align with Target Security Architecture? | |
| 5. Is the <i>software</i> capable of being managed and maintained with standard SNMP-based management tools? | |
| Total Rating Points | |

Please refer to http://www.azgita.gov/enterprise_architecture/NEW/Software_Arch/AppendixB.pdf for a listing of the Statewide Applications Software Table.

