UNM | Office of the CIO

UNM Application Development and Support Standard

IT Standard Issued: Draft of March 24, 2016
Effective Date:
Responsible Executive: UNM Chief Information Officer (CIO)
Responsible Office: UNM CIO
Contact: IT Director, Applications

Purpose of the Application Development and Support Standard

The purpose of an Application Development and Support standard is to outline the minimal characteristics of secure, available, consistent, and usable web, mobile and batch applications intended for use by UNM faculty, staff and students, as well as the external academic and administrative communities of instruction, research, suppliers, customers and potential students. The Application Development and Support Standard identifies the technical and support areas that need to be integrated in order to deliver effective applications to the UNM community.

What is Application Development and Support?

Application Development refers to all organizational resources applied to building applications from conception and design through deployment and maintenance. Applications encompass not only the user interface but also the system, platform, security and network infrastructure that capture information, delivery to the end-user and support of the application. Applications may collect, process, integrate and report on data/information; and content can be collected and delivered on paper, on the web, on desktop and/or on mobile devices for processing on local, centrally-managed or cloud environments.

Application Support refers to the organizational resources applied to using, sustaining, maintaining and extending the useful life of applications in the business context of the organization.

> **Example of application development and support**. The UNM Information Technologies department under the CIO (UNM IT) supports and manages core enterprise applications such as Banner. UNM IT also provides professional consulting and technical expertise in the development of non-core applications, mobile apps, and reporting systems, including review, analysis, integration, upgrade, maintenance and support[i]. See the UNM IT Service Catalog for application support related services. http://it.unm.edu/servicecatalog/asset_list.php?type=5&a_id=33&dept=637&origin=az.

Who is affected by the Application Development and Support Standard?

This Application Development and Support Standard applies to any UNM organizational entity (i.e. branch, division, college, school, department, business unit, or other UNM affiliated organization, including UNM IT), hereinafter referred to as a "department", that intends to implement, or has implemented UNM-developed, custom (contracted with a vendor) or commercial off-the-shelf (COTS) applications, or that supports or administers applications for the benefit of part or all of the UNM community.

Scope of the Application Development and Support Standard

The standard addresses the following Enterprise and Supplemental Services named by the IT Strategic Advisory Committee, which are all forms of application development and need to adhere to the criteria identified in this standard:

- Application Development
- Application Maintenance
- Mobile App Distribution
- Reporting and Report Development

Given the distributed nature of Application Development and Support and the potential for application development across the campus community, the standard assures continuity, reliability, and sustainability of apps used by and branded as UNM. The standard encompasses these aspects of application development and support:

- **Core development life cycle activities** related to the development of software (Requirements, Design, Construction, Testing, Debugging, Deployment or Transition to Operations and Maintenance).
- **All architectural/supporting technologies** (such as coding languages, database management systems, operating systems, frameworks, mark-up languages….) that scaffold the development environment. This includes the technical architecture or infrastructure, used to support the development and delivery of applications to end-users.
- **All application types**, for example data collection, transaction processing, reporting, mobile, packages, remotely-hosted, Applications as a Service, among others.

Excluded from the scope of the standard are:

- Non-interactive or static (informational) Web page development
- **Systems architecture**, which is the management domain of systems and networking infrastructure areas that enable application development on behalf of UNM.
- **Specific technologies used to in any aspect of application development**, such as servers, operating systems, compilers, backups, or network distribution software (iOS or Android, Java, Linux, Apache, Oracle, html, MySQL, php, for example).
- Specific **paradigms and models used in development for efficiency**, such as Software engineering, Waterfall, Spiral, Agile, Lean.
- **Specific development frameworks, software or team management approaches**, such as Scrum or Team Management Software.
- **Specific approaches or industry standards used to ensure quality or process improvement**, such as ISO 9000, Capability Maturity Model Integration or bodies of knowledge for software engineering or project management.
- **Specific** approaches used for **cross-tool visibility, integration, synchronization or reporting**, such as GUI designers, release automation, or APIs.
- **Areas addressed in other UNM standards or policies**, such as Data Center, Project Management standards, or the Information Security Program.

Responsibilities Concerning the Standard

- **Office of CIO**: Ensure currency, correctness and appropriate periodic review of the standard by facilitating review and update of the standard as needed.
- **Departments that develop applications**: Comply with the Application Development and Support Standard specifications below.

Process for Review of the Standard

The process to update the standard is defined and described on the Standards page of the CIO website at http://cio.unm.edu/standards/standards-development.html:

- Requests for review and update of the standard can be submitted to the Office of the CIO who facilitates the update. The CIO may independently, or upon request of the administration, also determine if review and update is appropriate for the standard.

Compliance

- This standard has been developed under and is subject to all UNM policies, some of which are cited in the References.
- The UNM Administration, Internal Audit, or UNM IT may determine the compliance of departmental support approaches with this standard.

Application Development and Support Standard Specifications

General Guidelines.

When evaluating whether to **develop an application in house, insource to another UNM department, or outsource to an external vendor for custom development or purchase commercial off-the-shelf (COTS) software,** the following factors should be outlined for UNM executives who will make the IT investment decision:

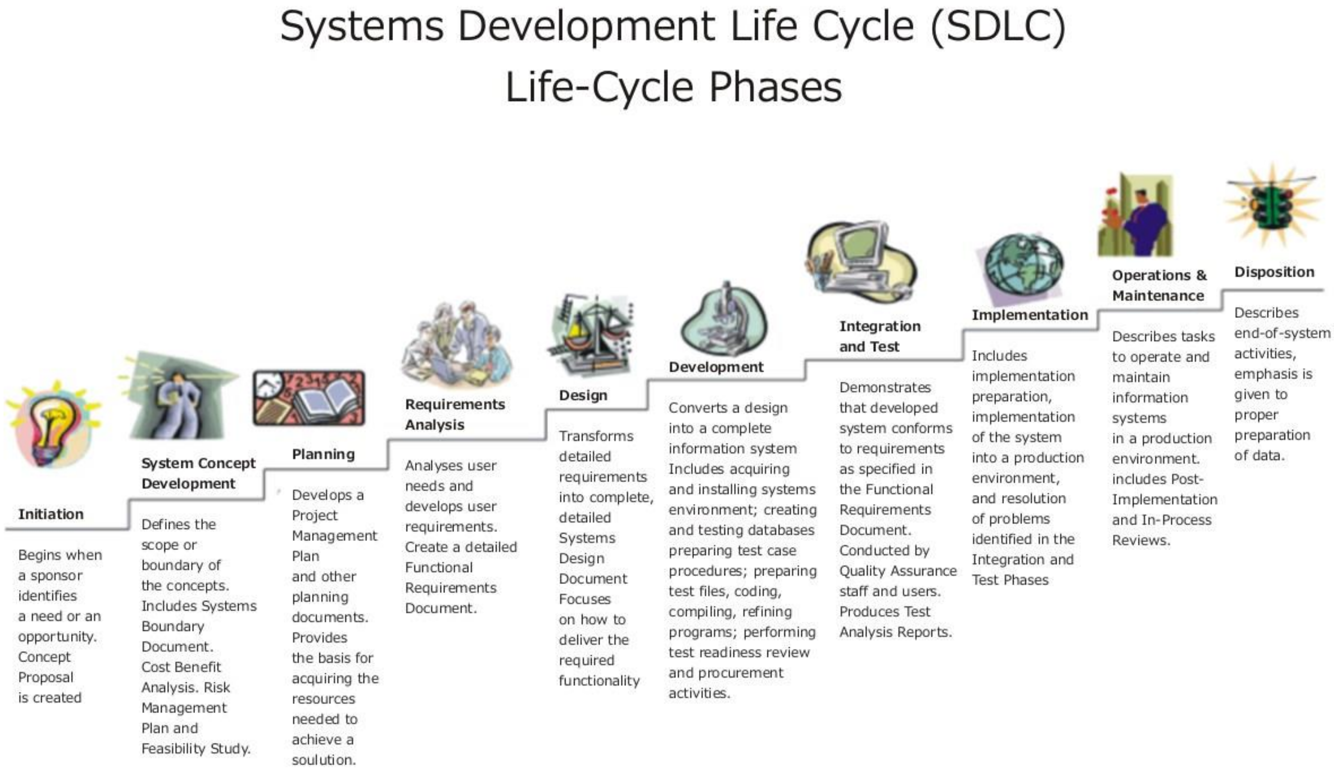
1) Cost of ownership to develop and support and application (one-time and recurring)
2) Appropriate stakeholder involvement in the development process
3) UNM Branding and naming of applications
4) Management and funding of licensing and maintenance agreements for software and hardware assets, including response to license audit requests
5) Management of business and technical relationships with the provider
6) Support for requests and incidents, as well as escalation paths
7) Integration with technology assets currently in use at the University
8) Training of user and technical staff
9) Scalability to other UNM departments or higher education partners in the State. This would include definition of an approach and support to on-board additional UNM and non-UNM users.
10) Appropriate ownership, access to, and security of University information
11) Appropriate security classification of information
12) Compliance with Business Associates Agreements (BAA)
13) Protection of personally-identifiable, or HIPAA- or FERPA-protected information
14) Adequate backup and recovery protocols
15) Appropriate Business Continuity protocols in the department
16) Technical and business expertise to maintain or upgrade the application
17) Processes for communication and system integrity when making changes or performing maintenance
18) Potential overlap or duplication with other applications
19) Availability of end-user documentation
20) Demise process for the application that would address disposition of data, including removing data from a vendor site and returning it to UNM.
21) Integration with other UNM-branded applications, especially enterprise applications, such as Banner
22) Functionality – expected duration of usefulness to the community intended to be served

Development Life Cycle

Departments developing or supporting applications need to follow development life cycle activities. Core activities of new application or system development and support life cycle (SDLC) integrate with Project Management phases when standing up any new application or making enhancements to existing applications. Development life cycle applies to all types of applications (data collection, processing or reporting) using any technology (web, mobile, mainframe, PC, cloud).

The chart[ii] below:

- Identifies steps for successful systems development, regardless of the infrastructure an application runs on, even if that infrastructure or the application itself is managed in the cloud.
- The chart speaks specifically to the application itself, and does not specifically address, but assumes, other work needed to align business processes with the application in the affected department(s), infrastructure changes, or documentation.
- The chart integrates project management practices applied in the development of an application. See the **IT Project Management Standard**, which specifies minimum documentation and artifacts required for projects, including projects that develop applications.



Systems Development Life Cycle (SDLC)
Life-Cycle Phases

Initiation
Begins when a sponsor identifies a need or an opportunity. Concept Proposal is created

System Concept Development
Defines the scope or boundary of the concepts. Includes Systems Boundary Document. Cost Benefit Analysis. Risk Management Plan and Feasibility Study.

Planning
Develops a Project Management Plan and other planning documents. Provides the basis for acquiring the resources needed to achieve a soulution.

Requirements Analysis
Analyses user needs and develops user requirements. Create a detailed Functional Requirements Document.

Design
Transforms detailed requirements into complete, detailed Systems Design Document Focuses on how to deliver the required functionality

Development
Converts a design into a complete information system Includes acquiring and installing systems environment; creating and testing databases preparing test case procedures; preparing test files, coding, compiling, refining programs; performing test readiness review and procurement activities.

Integration and Test
Demonstrates that developed system conforms to requirements as specified in the Functional Requirements Document. Conducted by Quality Assurance staff and users. Produces Test Analysis Reports.

Implementation
Includes implementation preparation, implementation of the system into a production environment, and resolution of problems identified in the Integration and Test Phases

Operations & Maintenance
Describes tasks to operate and maintain information systems in a production environment. includes Post-Implementation and In-Process Reviews.

Disposition
Describes end-of-system activities, emphasis is given to proper preparation of data.

- **Initiation.** A business opportunity, a problem to be solved, or a business or technical need is identified, which launches evaluation of options, costs, risks and benefits associated with an application development project. Awareness of the data involved in the application should be considered from the onset to ensure appropriate permission, security and protection, per the Data Governance link referenced below.
- **System Concept Development.** The business case is made for an approach to address the opportunity. The Business Case also identifies stakeholders and roles needed in the development process. See the IT Project Management Standard.
    - If COTS software is part of the concept, perform a security review before purchase. See https://unm.custhelp.com/app/answers/detail/a_id/7486/kw/purchasing%20review for related information.
- **Planning.** A project is defined and preliminary planning is outlined. This is the basis for acquiring resources to execute the project and achieve the goals of the project. See the IT Project Management Standard.
- **Requirements Analysis**. Analyze and document the existing environment and available applications, and identify alternative solutions to meet organizational objectives, their costs, benefits and drawbacks.
    - Requirements need to be achievable, specific, and clear, and include costs, stakeholder and end-user expectations, and governance expectations.

    - Functional stakeholders sign off on system requirements, which subsequently can be changed through scope management of the development project, unless otherwise specified.
    - Define and document acceptance criteria.
- **Design**. Describe and document features and operations in detail, addressing all layers of the architecture, including business rules and cases, and including logic or pseudocode.
    - **Current System Analysis** Review current system architecture, design, functions, features and code.
    - **Branding**. University Communications & Marketing review application naming and marketing plans in compliance with University Guidelines.
    - **Data flow.** Identify and document data flow end-to-end, where edits occur and edit routines, integration points between applications, required data security at access, capture, transition, storage and reporting.
        - Ensure data protection according to its classification. See http://data.unm.edu.
    - **Business Workflow Design.** Design business workflow surrounding the application.
    - **Technical Specification.** Logic and system flow is designed and specified for programming staff.
        - Define changes to application architecture. Plan and sequence architecture changes to support the application.
        - Define required availability, capacity, and continuity.
        - Define testing plans in alignment with acceptance criteria and requirements.
    - **Support Design**. Define support design for the application: knowledge management, service transition, Standard Operating Procedures (SOPs), incident handling, communication and escalation, and performance monitoring for the application.
    - **Communication Design**. Design the approach and plan to communicate with end-users, stakeholders for application development, testing and implementation.
    - **Training Design**. Design training required for end-users and technical maintenance staff. Outline application documentation.
    - **Liability.** University Counsel and Purchasing review vendor contracts, app distribution channels and the like that could have liability implications for the University.
    - **Security Review**. A security review is an essential component of design, requiring separate signoff. Security reviews address:
        - Application security (e.g., data access, capture, display, storage)
        - Database security (e.g., data isolation in multi-tenant environments)
        - Integration Security (protecting data used in multiple applications)
        - Hosted Data Management (data in, to and from remote data centers)
        - Hosted Security (virtual and physical in remote data centers)
        - Data Communication security (e.g., data in transit, data exchange)
    - New **business processes and transition to them**, marketing, architecture of the infrastructure, ADA compliance, among others, are part of design.
- **Development or Construction**. Plan and design are executed in this point of application development. Beyond coding to the above design, development may also include adding technical or security components to the infrastructure to support the application.
    - Code should be reviewed, managed and backed up.
    - Documentation should be embedded in code to ensure maintainability.
- **Integration and Test**.
    - Developers test and correct programming units, functional modules, module integration, interoperability, rendering on all browsers and mobile devices
    - Developers volume test for load on the network and servers.
    - Developers regression test to make sure that old code works with the new changes.
    - Developers test backup and recovery of data with the new modules.
    - End-user or functional experts check for coding or integration errors from beginning to end of a business process, according to requirements and acceptance criteria.
    - Developers correct coding or integration errors that are identified by end-users as a normal component of testing.

    - A final security review is required before implementation to validate that the security plan, security architecture or security specification has been properly executed.
- **Implementation or Deployment**. When end-users have formally accepted the functionality of the application, install or move the application to operation/production, so that users can begin using the application for its business purpose. The development project may complete or close when an application transitions to Operations, but the development life cycle continues through the life of the application.
- **Operation and Maintenance**. Maintenance ensures that the application does not become obsolete or inoperable. Maintenance includes administrative and technical tasks, as well as minor and major enhancements to the application. During this phase in the life cycle, patches are applied and upgrades are conducted, including continuous evaluation of performance in terms of security, performance efficiency, capacity, and availability / reliability. Define and publish routine maintenance windows, which may result in system unavailability. Maintenance that entails service interruption requires at least two-weeks' notice.
- **Disposition or Disposal**. Disposition addresses the demise of an application and removal from operations when it no longer is effective in meeting business needs.
    - End-users should be invited to provide input on the continued usability and usefulness of the application. When the application is to be demised, ensure that all stakeholders and users are notified.
    - UNM data that is transmitted to or stored in vendor locations should be returned to UNM and removed from the vendor site. The vendor should provide written confirmation of this action.
    - The disposal of any physical technology assets complies with University Policy for Asset Management.
- ***Minimum* artifacts** required for the Application Development Life Cycle include:
    - **Service Level Agreement or Contract** with the development provider (UNM or vendor provider) on the specifications, functionality and support of the delivered application.
    - **Required Project artifacts** when standing up the application (See IT Project Management Standard).
    - **Support artifacts** (See Service Desk Standard) including but not limited to end-user documentation, triage and troubleshooting scripts, management and technical escalation paths, maintenance windows for application unavailability, among others.

Infrastructure, Equipment and Upgrades

- Data Centers or server rooms comply with the **Data Center Standard** for physical security.
- Upgrade or refresh hardware and software **during breaks** in the semester or business cycle, or when an Application is offline so end-users are not negatively impacted.
- Infrastructure includes a **development instance and an operational instance** or environment used for development/testing and production processing. This includes but is not limited to operating systems, security patches, compilers, firewalls, databases, test and production data management, among others.
- In transitioning **changes to operations**, ensure that changes are approved, logged, scheduled, tested, migrated and that a back-out option is available in the event of an unsuccessful change. Changes that entail service interruption outside of the published maintenance windows require at least two-week advanced notice to users.
- **Storage strategies** for information assets address not only business data and information, but also address log files, cache files and other data generated by the application that will grow over time.
- **Data backup and recovery** strategies address all data and are tested whenever significant changes are made to data structures or processing rules.
- **Technical architecture** (servers, operating systems, development languages, database management, and access and security protocols, among others) is defined, documented and published for consistency and ease of use by application programmers.
- **Minimum Infrastructure** for applications:
    - **Data Center or Server room** in compliance with the Data Center Standard.
    - **Secure and current development and operations environments** in which to maintain the application without interrupting business use of the application.

    - **Backup and recovery processes** to ensure business continuity.

Support

- **Publicly identify whom to contact and when they are available for technical support** of an application for end-users and for administrators of the application. This includes technical on-call staff for incident (break/fix) handling.
- Provide online **documentation and triage scripts for trouble-shooting** end-user issues with an application.
- Integration with a **Service Desk** (see Service Desk standard) for end-user and customer support is desirable to consistently manage communication with end-users and IT staff. Logging, monitoring, escalating and tracking contacts, as well as reporting on end-user satisfaction with the service is part of Service Desk support.
- Technical and functional support roles for an application need to be identified, documented, and contracted with the application provider (UNM or vendor).
- Any support changes will require a review and update of related documentation.

Security

- Protected information needs to be secured appropriately for access, use, transit and storage. The Data Center Standard addresses physical security of server rooms. Developers need to address network and access security of data. See the Data Governance reference below.
- Application developers can refer to the **Application Evaluation Guide** on the CIO standards page cited in the References.
- **Minimum Security requirements** for Application Development and Support:
    - **Security Review** sign off as the application is moved into Operations. (See Project Management Standard)

Role and Responsibilities of Application Manager

- Ensure the integrity of the University's technology infrastructure, assets and services that underpin the Application, including connectivity, storage, end-user support and security.
- Provide information for end-users and timely support of anomalies and service interruption.
- Champion customer requirements for the deployment of new applications.

Role and Responsibilities of Stakeholders of Applications

- Report anomalies and things that don't work to the appropriate service provider.
- Ensure compliance with the approved IT standards.
- Protect the integrity of University information assets processed in applications
- Comply with University policies.

References

- **UNM Policy Manual Section 2500-2599**: Electronic Management Systems, especially 2500, Acceptable Computer Use: http://policy.unm.edu/university-policies/2000/2500.html; 2550 for Information Security: http://policy.unm.edu/university-policies/2000/2550.html; and Security Controls and Access to Sensitive and Protected Information 2520 http://policy.unm.edu/university-policies/2000/2520.html and Social Security Numbers, Policy 2030 https://policy.unm.edu/university-policies/2000/2030.html.
- **Application Evaluation Guide** http://cio.unm.edu/standards/docs/applications-evaluation-0906.pdf.
- **UNM Data Governance** http://data.unm.edu/,
- **FastInfo** UNM IT's Knowledgebase of frequently asked questions, especially the **Security Review for Purchasing Software** https://unm.custhelp.com/app/answers/detail/a_id/7486/kw/security%20assessment.
- **UNM Identity Standards** https://ucam.unm.edu/marketing/identity-standards.html.

- **Information Security Program,** http://it.unm.edu/security/program.
- **Accessibility/ADA guidelines** are offered by Accessibility Services for students http://as2.unm.edu/, and the Physical Plant https://iss.unm.edu/PCD/university-planning/facility-access-ada.html.
- **FERPA**. Guidance for complying with the Family Educational Rights and Privacy Act (FERPA) are provided by the Registrar: https://registrar.unm.edu/privacy-rights/ferpa.html.
- **IT Standards** and related processes and information cited in this document, including a link to the Application Evaluation Guidelines, can be found on the Chief Information Officer website: http://cio.unm.edu/standards/.

[i] Information Technologies Department Service Catalog for Application Support. http://it.unm.edu/servicecatalog/asset_list.php?type=5&a_id=33&dept=637&origin=az.

[ii] https://en.wikipedia.org/wiki/Systems_development_life_cycle.