Enterprise Architecture

Enterprise Architecture (EA) is a framework intended to provide a holistic view of the processes, data, application systems, and technology infrastructure. This view provides context for planning the evolution of institutional information systems into an integrated environment that is responsive to change and supports the delivery of the University strategy.

EA helps standardize technology solutions and tries to avoid implementing one-off applications that tend to be difficult to support. It also ensures that when new systems or applications are acquired there is consideration for interfaces, integrations, security, business continuity, and accessibility. Getting more visibility into all the technologies on campus will help eliminate duplication of applications.

Purpose of Principles

Enterprise Architecture Guiding Principles help create a unified vision to support all University technology and services that span the enterprise in how they are managed, acquired, designed, and configured. These principles should reinforce other efforts across campus, such as the Change Advisory Board (CAB), Data and Business Process Advisory Committee (DBPAC), Strategic Project Review and Resourcing Committee (SPRRC), etc.

Principles align information system uses and development with the University's mission, strategic objectives, and goals. This acts as a mechanism for consistent decision making across units. Deviating from the principles may result in unnecessary long-term cost and risk.

Use of Principles

Architecture principles should always be considered when making any decision regarding the use, selection, evolution, and integration of all information systems resources and assets at the University. These principles are inter-related and need to be applied as an interconnected set. There may be times when principles are not in harmony which will require a decision as to which principle will take precedence on a particular issue. The rationale for such decisions should always be documented to inform future decisions on the initiative.

NAU Architecture Principles

Maximize Benefit

Strategic decisions regarding information systems must always strive to provide maximum benefit to the institution, align with NAU's stated mission, vision, and values, while balancing the long-term costs and risks.

Rationale: Every strategic decision must be assessed from a cost, risk, and benefit perspective. Decisions based on requirements defined by university strategic planning, as opposed to those made at departmental levels have greater long-term value. No one group or area will detract from the benefit to the enterprise. However, this principle will not preclude any of those groups or areas from receiving support towards achieving their objectives.

Implications:

- Adherence to this principle will result in:
  - Process improvement before information system change. Evaluating business processes may result in efficiencies that would not require an information system change.
  - Reuse before buy. Wherever possible, existing systems and technology should be used.
  - Configuration before customization. Information systems that are adaptable to changing business processes may cost more initially but reduce the long-term costs and risks associated with customization.
  - Buy before build. Commercial off-the-shelf (COTS) systems may be acquired instead of custom development where a suitable solution is available.
  - Due to the high support cost, custom built solutions will only be considered when other options have been exhausted.
- Must ensure the benefits outweigh the costs and risks associated with the initiative.
- Costs must be determined based on the total cost-of-ownership (including both business and IT cost) across the lifecycle of the initiative.
- To maximize benefit, departments may have to concede their preferences for the benefit of the entire university.
- Information system initiatives should be conducted in accordance with the University strategic plan.
- Information systems should be designed to allow for enterprise-wide use, rather than use by one department.

Control Technical Diversity

Technological diversity must be controlled in order to minimize the cost of maintaining expertise in, support of, and connectivity between multiple information system environments.

Rationale: There is a substantial cost related to the infrastructure required to support information systems. There are additional costs required to integrate, maintain, and support information systems running on multiple, and occasionally inconsistent, platforms. Technical administration and support costs are better controlled when limited resources can focus on shared set of technology. The business advantages of minimal technical diversity include greater flexibility to accommodate technological advances.

Implications:

- Technology platforms must be identified and documented. Additionally, recurring analysis needs to be done that rationalizes the existing diversity.
- Policies, standards, and procedures that govern the acquisition of technology must be tied directly to this principle.
- Technology choices will be constrained by the choices available within the technology architecture. Procedures for changing the technology standards to meet evolving requirements will have to be developed and implemented.

Risk-Based Approach to Security

Information systems, data, and technologies must be protected from the risk of unauthorized access, loss, or other adverse circumstance that may have a negative impact on University objectives.

Rationale: Risk is the possibility of loss, injury, or other adverse circumstance that, if it does occur, will have a negative impact on university objectives. Risk assessment is the overall process of risk identification, analysis, evaluation, and mitigation.

Following a risk-based approach provides the University with an opportunity to:

- Identify risks to projects, initiatives, data, and the ongoing operation of information systems.
- Effectively allocate and use resources to manage those risks.
- Improve stakeholder confidence and trust.

Implications:

- The risk to data and information systems must be assessed in order to achieve an acceptable level of confidentiality, integrity, and availability.
- University information must be safe-guarded against inadvertent or unauthorized alteration, sabotage, disaster, or disclosure.
- The cost and level of safeguards must be taken into consideration when implementing or modifying controls. Mitigation of risk will be weighed against the value of the assets and the consequence and the likelihood of the risk occurring.
- Options for addressing the risk should be reviewed and the decision about treatment of the risks documented.

Data is an Asset

Data is an asset with value to the University and needs to be managed accordingly.

Rationale: Data is a resource that has real, measurable value. It is the foundation for decision making and an enabler of improved business process, agility, and innovation. Carefully curating and managing data ensures that we can rely on its accuracy and is available when needed.

Implications:

- This is one of two closely related principles that align with the University Data Classification and Handling policy.
- Procedures must be developed and used in order to prevent and correct data errors and to improve processes that produce incorrect data.
- Data quality will need to be measured and steps must be taken to improve data quality.

Data is a Shared, Available Resource

Data is captured once and shared across university functions and units.

Rationale: Availability of information must be considered from an enterprise perspective in order to allow appropriate access by a wide variety of users. Timely access to accurate data is essential to improving the quality and efficiency of University decision-making and supporting academic, research, and administrative activities. It is less costly to maintain accurate data in a single application and share it, than it is to maintain data in numerous applications with differing rules and disparate management practices.

Implications:

- This is one of two closely related principles that align with the University Data Classification and Handling policy.
- The University must adopt common methods and tools for creating, maintaining, and accessing the data shared across the institution.
- The University must adopt and enforce common data access policies and guidelines for information systems to ensure that data remains available to the shared environment and that data can continue to be used by new initiatives.
- Availability involves making data discoverable while adhering to the need to restrict the access to classified, proprietary, and sensitive information.

Common Vocabulary and Data Definitions

Data is defined consistently throughout the University and the definitions are understandable and available to all users.

Rationale: The data that will be used in the development of information systems must have a common definition throughout the University community to enable the sharing of data. A common vocabulary will facilitate communications and enable effective dialog. In addition, it is required to interface systems and exchange data.

Implications:

- The University community must establish a common vocabulary, availability guidelines, sensitivity labeling, and business rules about the data. The data definitions will be used uniformly throughout the institution.
- Whenever a new data definition is required, the definition effort will be coordinated and reconciled with the University 'glossary' of data descriptions that will need to be established.

Ease-of-Use

Applications need to be intuitive. The technology should be transparent to users, so they can concentrate on their objectives rather than on their interaction with the system.

Rationale: For University community members, using different applications should be as intuitive as driving cars of different makes. The more a user must understand the underlying technology, the less productive that user is. Consistent user experiences are an incentive for use of applications. The knowledge required to operate one system will be similar to others. Training can be kept to a minimum and the risk of mistakes or misuse is reduced.

Implications:

- Applications that are used infrequently shouldn't require significant re-learning to carry out a task.
- This principle should apply to vendor products, as well as applications developed in-house.
- Common look and feel standards must be designed in order to be adaptable to the environment they operate in and must evolve. Effort should be made to evaluate and enhance the look and feel.
- Guidelines for user interfaces should not be constrained by narrow assumptions about user device, location, language, technology experience, or physical capability.

Requirement Based Change

Changes to applications and technology are only made when justified by business needs.

Rationale: This principle promotes an atmosphere where the information systems change to reflect the business goals, rather than changing the business because of information technology changes. This ensures that business needs are the basis for a proposed change and that involuntary effects on the business, resulting from information technology changes, are minimized. Technological improvements and advancement will present opportunities to evaluate business processes and subsequently alter business needs.

Implications:

- This principle ensures that the practice of turning on additional functionality merely because it is available does not occur.
- A technical improvement or system development will not be implemented unless a documented business need exists. Ensuring our systems are secure and up-to-date is a business need.
- The business need must be considered but it must also be aligned with other enterprise architecture principles. There must be a balance between business needs and information system operations and maintenance.

Responsive Change Management

Changes to the enterprise information environment are implemented and documented in a timely manner.

Rationale: If people are working within the enterprise information environment, then that information environment must be responsive to their needs.

Implications:

- There must be a process for managing and implementing changes that do not create unnecessary delays.
- A user who identifies a need for change will need to connect with the appropriate resource in order to facilitate explanation and implementation of that need.
- Related user and technical documentation must be kept up to date.