UNIVERSITY OF SASKATCHEWAN

Enterprise Architecture Principles

Information and Communication Technology

Introduction

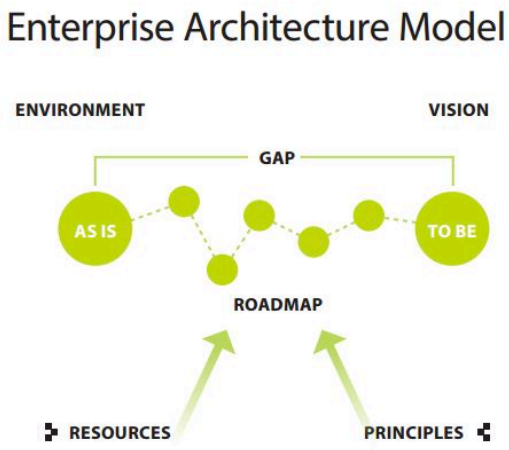
The university's vision uses enterprise architecture to provide a holistic view of the processes, data, application systems and technology infrastructure that exists within the University of Saskatchewan. This holistic view, or blueprint, provides strategic context for planning the evolution of institutional information systems into an integrated environment that is responsive to change and supports the delivery of university strategy.

The principles defined in this document form the basis for governance of the University of Saskatchewan's enterprise architecture.

Purpose of Principles

Principles are statements of direction that provide a foundation for decision making in the selection, implementation and evolution of the university's information systems. Enterprise architecture principles align information system uses and development with the university's mission, strategic objectives and goals.

Enterprise architecture principles serve as a framework for decision making by providing guidance about the preferred outcomes of a decision in a given context. This acts as a mechanism for harmonizing decision making across units and guiding the selection and evolution of information systems to be as consistent and cost effective as possible.



Use of Principles

Enterprise architecture principles should be considered when making any decision regarding the use, selection, evolution and integration of all information systems resources and assets at the University of Saskatchewan. These principles are inter-related and need to be applied as a cohesive set. Each principle must be considered in the context of "all other things being equal". There are times when a decision will need to be made regarding which principles will take precedence on a particular issue. When those situations arise, the rational for the decision needs to be recorded. The recorded rational will be used to inform future decisions on the initiative and allow for the consistent application of the principles.

Governance of the Principles

These principles provide guidance and direction for the use and evolution of information systems. Deviating from the principles may result in unnecessary and avoidable long-term costs and risks.
As such, deviation from the solution-set bound by these principles requires the **explicit** approval of the Information Systems Steering Committee (ISSC) through its designated Architectural Governance process.

How do Enterprise Architecture Principles fit within the Institution

Alignment with enterprise architecture principles should be a goal for any initiative and will result in fewer obstacles, surprises and course corrections later in the project. To achieve these benefits, a review of the alignment between the initiative and enterprise architecture principles must be done in advance of a charter review by any ICT Steering committee.

Summary of the Principles

The following principles apply to all decisions made at the university regarding information system change. Although they apply to all personnel, they will most frequently be used by those responsible for designing technology-enabled solutions.

General Principles

1. Principled Decision Making
2. Maximize Value to the University
3. Maintain Transparency in Information System Decision Making
4. Plan for Continued Operations
5. Minimize Duplication
6. Maintain Legal and Regulatory Compliance
7. Risk-based Approach to Security
8. Information Systems Responsibility
9. Continuous Improvement

Data Principles

10. Data is an Asset
11. Data is a Shared Resource
12. Common Vocabulary and Data Definitions
13. Data is Easily Accessible
14. Data Manager

Application Principles

15. Convergence With the Enterprise Architecture
16. Enterprise Architecture Applies to External IT providers
17. Technology Independence
18. Ease-of-Use
19. Component Simplicity and Reusability
20. Reusable Interfaces

Technology Principles

21. Requirement Based Change
22. Responsive Change Management
23. Control Technical Diversity
24. Seamless Integration

General Principles

Principle 1: Principled Decision Making

Statement:

The information systems principles apply throughout the university and take precedence over all other considerations when information system decisions are made.

Rationale:

These principles provide guidance and direction for the use and evolution of information systems. Deviating from the principles may result in unnecessary and avoidable long-term cost and risk.

The only way we can provide a recognized, consistent and measurable level of operations is if all organizational units within the university abide by the principles when making decisions.

Implications:

- Without these principles, short-term considerations, convenient exceptions and inconsistencies will rapidly undermine the management of information systems.
- Information system initiatives will not begin until they are examined for compliance with the principles.
- Principles are inter-related and need to be applied as a cohesive set. Initiatives that are in conflict with the principles require the **explicit** approval of the Information Systems Steering Committee (ISSC) through its designated Architectural Governance process.

Principle 2: Maximize Value to the University

Statement:

Strategic decisions for information systems must always strive to provide maximum value to the institution while balancing the long-term costs and risks.

Rationale:

Every strategic decision must be assessed from a cost, risk and benefit perspective. Decisions made from a university-wide perspective have greater long-term value than decisions made from any particular organizational unit's perspective.

Maximizing the benefit to the university requires that information system decisions adhere to enterprise-wide drivers and priorities. No group will detract from the benefit of the whole; however, this principle will not preclude any group from getting their job done.

Implications:

- We need to ensure the quantitative and qualitative benefits outweigh the costs and risks associated with the initiative.
- The costs must be determined based on the total cost-of-ownership across the lifecycle of the initiative. This includes business costs as well as information system costs.
- This will often result in:
    - Reuse before buy. Wherever possible, existing systems and technology should be used rather than acquiring or developing a new system.
    - Buy before build. Open source systems or commercial off-the-shelf (COTS) systems should be acquired instead of in-house development where a suitable solution is available that is not cost prohibitive.

    - Configuration before customization. Information systems that are adaptable and flexible to changing business processes may cost more initially but reduce the long term costs and risks associated with customization.
    - These considerations need to be balanced with the minimize duplication principle and the convergence with the enterprise architecture principle.
- Achieving maximum enterprise-wide benefits will require changes in the way we plan and manage information systems. Technology alone will not bring about change.
- To maximize utility, some units may have to concede their preferences for the benefit of the entire university.
- Information system initiatives should be conducted in accordance with the information systems strategic plan. Individual units should pursue information system initiatives which conform to the blueprint and priorities established by the university. The strategic plan will change if it needs to.

Principle 3: Maintain Transparency in Information System Decision Making

Statement:

All organizational units at the university participate in information systems decisions needed to accomplish business objectives.

Rationale:

Information system users are the key stakeholders and customers in the application of technology to address a business need. In order to ensure information systems align with the business, all organizational units in the enterprise must be involved in all aspects of the information environment. The subject matter experts from across the enterprise and the technical staff responsible for developing and sustaining the environment need to come together as a team to jointly define the goals and objectives of information systems.

Implications:

- To operate as a team, all stakeholders and customers will need to accept responsibility for developing the information environment.
- Resource commitment will be required to implement this principle.
- Risk is managed jointly.
- Governance body decisions need to be widely communicated to ensure a shared understanding.

Principle 4: Plan for continued operations

Statement:

University operations must be maintained, despite system interruptions.

Rationale:

Information system operations are pervasive and we are dependent on them. Therefore, we must consider the reliability of such systems throughout their design, use and decommissioning.

Business units throughout the university must be able to conduct their normal operations, regardless of external events. Hardware failure, natural disasters and lack of data integrity must not stop business activities.

Organizational units must be capable of operating on alternative information delivery mechanisms.

Implications:

- Applications must be assessed for criticality and impact on the university's mission in order to determine the level of continuity that is required as well as what corresponding recovery plan is necessary. This includes identifying fallback modes of operation if available.
- Managing the ongoing operational risk includes, but is not limited to:
  - Regular system patching and updates
  - Regular testing for vulnerability and exposure
  - Periodic reviews or system audits
- Recoverability, redundancy and maintainability should be addressed at the time of design.
- The risk associated with running an alternative or fallback delivery model needs to be identified and remediated to an acceptable level.

Principle 5: Minimize Duplication

Statement:

Information systems should be designed to allow for enterprise-wide use, rather than use by a specific organizational unit.

Rationale:

Duplicating a capability is expensive and leads to inconsistent business activities and conflicting data.

Implications:

- Technology and services should not be duplicated when the need being fulfilled is the same.
- The impetus for adding to the set of university-wide capabilities may well come from an organizational unit making a convincing case, but the resulting capability will become part of the enterprise-wide system and the data it produces will be shared across the institution.
- Units are not permitted to develop capabilities for their own use which are similar to, or are a duplication of an enterprise-wide capabilities. This way, expenditures of scarce resources to develop essentially the same capability in marginally different ways will be reduced.
- If the enterprise capability is incomplete or deficient, efforts will be made to address the deficiency. This will allow us to achieve maximum utility from existing investments.
- When duplicate services or technologies exist, an effort to standardize on a single enterprise solution should be made. This principle may be influenced by the convergence with the enterprise architecture principle.
- Data and information used to support university decision-making will be standardized to a much greater extent than previously.

Principle 6: Maintain Legal and Regulatory Compliance

Statement:

Information system management processes must comply with all relevant contracts, laws, regulations and policies.

Rationale:

The university is subject to provincial and federal laws and regulations. There are however, additional laws, regulations, contracts, policies and standards that must be adhered to as a result of specific business activity within the university. Examples include, but are not limited to, Payment Card Industry standards (PCI), Canadian Anti-Spam Law (CASL), college accreditation standard and the university's Freedom of Information and Protection of Privacy Policy.

This principle will not preclude process improvements that lead to changes in internal policies and regulations.

Implications:

- The information system decisions must be mindful to comply with laws, regulations, as well as internal and external policies regarding the collection, retention and management of data.
- Staff need to be educated about the importance of regulatory compliance and their responsibility to maintain it.
- Where existing information systems are non-compliant they must be strategically brought into compliance.
- Change in law or regulation may drive change in our processes or applications.
- The information system decisions must be mindful contractual obligation.

Principle 7: Risk-Based Approach to Security

Statement:

The risk to information and information systems must be assessed to ensure an acceptable level of confidentiality, integrity and availability is achieved.

Rationale:

Risk is the possibility of loss, injury or other adverse or unwelcome circumstance that may 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 threats to projects, initiatives, data and the ongoing operation of information systems.
- Effectively allocate and use resources to manage those risks.
- Avoid unwarranted speculation, misinterpretation and inappropriate use.
- Improve stakeholder confidence and trust.

Implications:

- Information systems, data and technologies must be protected from unauthorized access and manipulation. University information must be safe-guarded against inadvertent or unauthorized alteration, sabotage, disaster or disclosure.
- The cost and level of safeguards and security controls must be appropriate and proportional to the value of the information assets and the severity, probability and extent of harm.
- Risk identification must take into consideration existing controls, 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.
- Risk treatment will typically involve choosing one or more of the following:
    - Accepting risk by having an appropriate university official sign off on the acceptance of the risk.
    - Avoiding risk by deciding not to pursue a particular initiative.
    - Transferring risk by having an appropriate university official transfer the risk to an external entity (such as by buying insurance).
    - Mitigating risk by applying appropriate safeguards and controls, and accepting the residual risk.
- Risk management related to data:
    - Sensitivity and risk must be assessed at the data level, not the application level.

- Aggregation of data, both sensitive and not, may result in new risks requiring a review to ensure the appropriate levels of control. Data stewards and/or subject matter experts must determine whether aggregation results in an increased sensitivity.
- Data safeguards such as restricting access to "view only" or "never see" should be considered. Sensitivity labeling must be determined.

Principle 8: Information Systems Responsibility

Statement:

The Chief Information Officer (CIO) is accountable for all information systems at the university through both an official role as well as the expectation of senior executive.

This accountability extends to the development and management of information systems and infrastructure that meet user-defined requirements for functionality, service levels, costs and delivery time.

Rationale:

The university is transforming into a digital enterprise where technology is both pervasive and ubiquitous. In this highly complex and distributed environment, it is essential to align expectations with capabilities and costs so that all information system initiatives are efficient, effective, have reasonable costs and clear benefits.

Implications:

- Governance and need identification processes must evolve that allow for the rationalized development and prioritization of information system initiatives and projects.
- Managing business unit expectations is critical.
- Business process, data, application and technology models must be created to allow us to understand the complex relationship between business processes and information systems.

Principle 9. Continuous Improvement

Statement:

All processes are in need of continuous improvement to stay relevant.

Rationale:

The rate of change and improvement in the worldwide information technology market has led to extremely high expectations regarding quality, availability and accessibility. As a result, ICT must deliver projects and service-level agreements (SLAs) on progressively shorter deadlines and information systems with increasingly higher quality in an effective cost-control manner.

This demand requires an operating model that continuously reviews and improves upon current practices and processes.

Implications:

- Performance metrics linked to business goals must be defined and used to drive improvements. Industry benchmarks should be used as a comparator where appropriate.
- Routine tasks that can be automated should be, but only where the benefit justifies the cost. The complexity of the process, the potential time savings and the potential for error reduction should be factored into the benefit.
- Processes and tasks must be analyzed and understood to determine the opportunity for improvement and automation.

- ICT staff must be increasingly qualified and motivated to automate their tasks as well as those of the business users.
- The standard information system and technology architectures must be defined and applied.
- Service outages, errors and problems need to be analyzed to understand and improve upon deficiencies in existing processes and practices.
- Manual integration, where data is copied from one information system to another by hand, should give way to automated processes that are repeatable, timely and less prone to error.

Data Principles

Principle 10: Data is an Asset

Statement:

Data is an asset that has value to the university and needs to be managed accordingly.

Rationale:

Institutional data is among the university's most valuable assets and represents a significant investment of time and effort.

Data is the foundation of our decision making, and supports academic, research and administrative functions. Therefore we must carefully manage data to ensure that we know where it is, so we can rely on its accuracy and obtain it when and where it is needed.

Implications:

- This is one of three closely-related principles that align with the University Data Management, Data Access and Data Use Policies. The implication is that there is an education task to ensure that all units within the university understand the relationship between value of data, sharing of data and accessibility to data.
- Stewards must have the authority and means to manage the data for which they are accountable.
- The role of a data steward is critical because obsolete, incorrect or inconsistent data could be passed to university personnel and adversely affect decisions across the institution.
- As defined by the Data Management Policy, the data steward is required to ensure data quality is sufficient for the institutional needs and not just the needs of the unit.
    - Procedures must be developed and used to prevent and correct errors in the information and to improve those processes that produce flawed information.
    - Data quality will need to be measured and steps taken to improve data quality.
    - Policy and procedures may need to be amended to ensure quality issues are addressed in a timely manner.

Principle 11: Data is a Shared Resource

Statement:

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

Rationale:

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 timely, accurate data and share it from a single application than it is to maintain duplicate data in multiple applications with multiple rules and disparate management practices. The university holds a wealth of data, but it is stored in hundreds of incompatible stovepipe information systems. The speed of data collection, creation, transfer and assimilation is driven by the ability of the university to efficiently share these islands of data across the institution.

A shared data environment will result in improved decision making and support activities as we will rely on fewer sources (ultimately one) of accurate and timely managed data.

Implications:

- This is one of three closely-related principles regarding data that align with the University Data Management, Data Access and Data Use Policies. The implication is that there is an education task to ensure that all units within the university understand the relationship between value of data, sharing of data and accessibility to data.
- In the short-term, we must invest in software capable of migrating legacy system data into a shared data environment to preserve our significant investment in legacy systems.
- We need to develop standard data models, data elements and other metadata that defines this shared environment and develop a repository system for storing this metadata to make it accessible.
- In the long-term, as legacy systems are replaced, we must adopt and enforce common data access policies and guidelines for information system initiatives to ensure that data remains available to the shared environment and that data can continue to be used by the new initiatives.
- For both the short-term and the long-term we must adopt common methods and tools for creating, maintaining and accessing the data shared across the institution.
- Data sharing will require a significant cultural change.
- This principle of data sharing will need to be balanced with the principle of data security. Under no circumstance will the data sharing principle cause confidential data to be compromised.
- Data made available for sharing will have to be relied upon by all users to execute their respective tasks. This will ensure that only the most accurate and timely data is relied upon for decision making. Shared data will become the university-wide 'virtual single source' of data. Energy and resources must be committed to this task

Principle 12: Common Vocabulary and Data Definitions

Statement:

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 dialog to be effective. In addition, it is required to interface systems and exchange data.

Implications:

- This principle is in alignment with the current University Data Management, Data access and Data Use Policy.

- The university community must establish a common vocabulary, accessibility 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. The Reporting and Data Services staff will provide this coordination and the repository for the glossary.
- Ambiguities resulting from multiple definitions of data must give way to accepted enterprise-wide definitions and understanding.
- Multiple data standardization initiatives need to be coordinated.
- Functional data administration responsibilities must be assigned.

Principle 13: Data is Easily Accessible

Statement:

Data must be accessible in order for university personnel to perform their functions.

Rationale:

Wide access to data leads to efficiency and effectiveness in decision-making and affords timely responses to information requests and service delivery. Access to information must be considered from a university-wide perspective to allow access by a wide variety of users. Staff time is saved and data consistency is improved.

Implications:

- This is one of three closely-related principles regarding data that align with the University Data Management, Data Access and Data Use Policies. The implication is that there is an education task to ensure that all units within the university understand the relationship between value of data, sharing of data and accessibility to data.
- Accessibility involves the ease with which users obtain information. Barriers to access should be removed where reasonable.
- The way information is accessed and displayed must be sufficiently adaptable to meet a wide range of user's needs and methods of accessing the data.
- Access and use of data requires an understanding of the data. It is the responsibility of every data user to understand the data that they use and to guard against making misinformed or incorrect interpretations of data or misrepresentations of information.
- Access to data does not grant the user rights to modify or disclose the data. Avoiding these common issues will require an education process and a change in culture, which currently supports a belief in 'ownership' of data by functional units.

Principle 14: Data Custodian

Statement:

Each data element has a Data Custodian accountable for data quality.

Rationale:

One of the benefits of an architected environment is the ability to share data across the institution. As the degree of data sharing grows and organizational units rely upon common information, it becomes essential that only the data custodian makes decisions about the content of data.

Note: A data custodian is different than a data steward. A data custodian is responsible for accuracy and currency of the data, while responsibilities of a data steward are broader and include data standardization, access, use and data definition tasks.

Implications:

- It is essential to identify the authoritative source of the data in order to identify the owner of the data and the management and stewardship responsibility.
- The data custodian will be responsible for meeting quality requirements levied upon the data for which the manager is accountable.
- Information should be captured once and immediately validated as close to the source as possible. Quality control measures must be implemented and adhered to, to ensure the integrity of the data.
- As a result of sharing data across the enterprise, the data steward is accountable and responsible for the accuracy and currency of their designated data element(s) and must recognize the importance of this responsibility.

Application Principles

Principle 15. Convergence with the Enterprise Architecture

Statement:

The convergence with enterprise architecture is valued and promoted as part of the institution's investment strategy.

The convergence with the enterprise architecture takes place strategically as new applications are built, new technologies are implemented and older systems are updated or decommissioned. Exceptions to the enterprise architecture may be supported for specific cases with **explicit** approval of the Information Systems Steering Committee (ISSC) through its designated Architectural Governance Process if the benefits of using a solution exceed those arising from the adoption of the enterprise architecture.

Rationale:

Convergence offers several advantages:

- It allows the enterprise architecture to evolve and accommodate changes in business and technologies.
- It avoids conversions of obsolete systems, which are extremely expensive.
- Over time, it preserves and rationalizes the investment in institutional systems.

Implications:

- Requires an architectural vision (As-Is vs To-Be) at the strategy, portfolio or capability level.
- Delayed convergence could reduce the benefits of the enterprise architecture.
- Requires a realistic and tangible approach to migration to the enterprise architecture and architectural standards.
- Requires an explicit transition strategy for current systems after the desired target architecture is identified.
- Allows decommissioning of an information system when appropriate.
- Requires a business case for exceptions, an exception process and an exit strategy. It must establish temporary or permanent exceptions, as well as exit strategies for temporary exceptions.
- Requires sponsorship to replace obsolete technologies.
- The One I.S. principles are a part of enterprise architecture and help guide the convergence based on responsible decision making.

Principle 16. Enterprise Architecture Applies to External IT Providers

Statement:

Outsourced activities must not be exceptions to the enterprise architecture simply because they are provided by a third party.

As outsourcing contracts and agreements are entered into, they must reflect and incorporate the One I.S. principles.

Rationale:

To be successful, enterprise architecture must be integrated with all information system projects and operational change activities.

Implications:

- Work needs to be done to inform procurement areas on enterprise architecture issues and develop practices that ensure these considerations are addressed.
- This requires partnerships and efficient communication between the business unit, procurement and information technology areas to get the benefits offered by the enterprise architecture.
- Information technology acquisitions must include requirements based on the enterprise architecture.

Principle 17: Technology Independence

Statement:

Application architecture must be planned to reduce the impact of technology changes and vendor dependence on the business. Applications are independent of specific technology options and therefore can operate on a variety of technology platforms.

Rationale:

Every decision made with respect to technology makes us dependent on that technology, therefore, the intent of this principle is to ensure that information systems are not dependent on specific hardware and operating systems software.

Independence of applications from the supporting technology allows applications to be developed, upgraded and operated under the best cost-to-benefit ratio. Otherwise technology, which is subject to continual obsolescence and vendor dependence, becomes the driver rather than the user requirements themselves.

Implications:

- Adherence to this principle requires consideration be given to whether an information system can support interchangeable technology components such as:
  - Web browsers
  - Operating systems
  - Physical and virtual hardware
  - Network components
  - Cameras
  - Projectors
- Application Program Interfaces (APIs) will need to be developed to enable legacy applications to inter-operate with applications and operating environments developed under the enterprise architecture.

- Middleware should be used to de-couple applications from specific software solutions.
- This principle also implies that technology standards be documented and metrics established to better understand operational cost. Adopting industry benchmarks should provide comparator metrics for efficiency and return on investment.

Principle 18: Ease-of-Use

Statement:

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

Rationale:

Using different applications should be as intuitive as driving cars of different brands.

The more a user has to understand the underlying technology, the less productive that user is. Ease-of-use is a positive incentive for use of applications.

The knowledge required to operate one system will be similar to others. Training is kept to a minimum and the risk of mistakes or misuse is reduced.

Implications:

- Systems that are only used occasionally shouldn't require significant re-learning in order to carry out a task.
- This does not just apply to the web-based applications.
- Applications must strive for a common look and feel.
- Common look and feel standards must be designed to be adaptable to the environment they operate in and must evolve. Effort should be made to measure and optimize 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.

Principle 19. Component Simplicity and Reusability

Statement:

The information system architecture is built with modular, reusable (plug-n-play) components that implement services.

Information systems architecture must be as simple as possible to meet changing business requirements. Whenever complexity is required, it must be abstracted to promote simplicity.

Rationale:

Reusable components represent opportunities to reduce information system development times and costs because they leverage investments in current systems. Modular components increase the system's capacities to adapt to different evolution needs, because the change is isolated from the affected modules.

Implications:

- The architecture establishes standards and guidelines to develop system components.
- Need to develop and publish a shared component library or catalog.
- Components may include but are not limited to:
    - Authentication services and authentication libraries

    - Authorization and rights management services
    - List services
    - Common look and feel styling repositories
    - Common code libraries and repositories
- Information system architecture is built over loosely coupled, modular, reusable components that implement services.

Principle 20. Reusable Interfaces

Statement:

Information systems must interact with each other through reusable interfaces that are self-described and minimize the impact of change.

Rationale:

Reusable interfaces are potentially consumable by more than one information system and safeguard against changes that cause a ripple effect into the consuming systems.

Implications:

- The technical approach leveraged to accommodate this principle may change over time as a result of changing technology practices.
- Training or education may be required to transition away from the current practice of developing point-to-point solutions.
- It will improve both the speed with which information system integration can be achieved and reduce the risk associated with change in the integrated institutional environment.
- Reusable interfaces mean that services are conceived in a way that generalizes specific consumer needs to allow for reuse by other systems with similar needs. This avoids the long term proliferation of interfaces resulting from creating an interface for each consumer and each specific need.

Technology Principles

Principle 21: Requirement Based Change

Statement:

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

Rationale:

This principle promotes an atmosphere where the information systems environment changes to reflect the business goals, rather than changing the business as a result of information technology changes.

This ensures that business operation 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 may generate opportunities to improve the business process and subsequently alter business needs.

Implications:

- This principle addresses the desire to turn on additional technological capabilities solely because they are available through a vendor technology bundle or as a throw-in on a licensing agreement.
- A technical improvement or system development will not be implemented unless a documented business need exists.

- Change management processes will need to conform to this principle.
- This principle may conflict with the responsive change management principle. 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.

Principle 22: Responsive Change Management

Statement:

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

Rationale:

If people are to be expected to work within the enterprise information environment, that information environment must be responsive to their needs.

Implications:

- We need to develop processes for managing and implementing changes that do not create delays.
- A user who identifies a need for change will need to connect with a subject matter expert (SME) to facilitate explanation and implementation of that need.
- If we are going to make changes, we must keep the architectures updated.
- Adopting this principle may require additional resources.
- Processes may need to be developed to manage priorities and expectations.
- This principle will, at times conflict with other principles. When this occurs, the business need must be considered but initiatives must also be balanced with other enterprise architecture principles. Without this balanced perspective short-term considerations, supposedly convenient exceptions and inconsistencies, will rapidly undermine the management of information systems.

Principle 23: Control Technical Diversity

Statement:

Technological diversity is controlled to minimize the non-trivial cost of maintaining expertise in and connectivity between multiple information system environments.

Rationale:

There is a real and significant cost related to the infrastructure required to support information systems. There are additional costs required to integrate and maintain information systems running on multiple, and occasionally inconsistent, infrastructures.

Limiting the number of supported components will simplify maintenance and reduce costs.

The business advantages of minimal technical diversity include:

- Standard packaging of components
- Predictable implementation impact
- Predictable valuations and returns
- Greater flexibility to accommodate technological advances
- Fewer service outages and lower training costs

Common technology across the enterprise brings the benefits of economies-of-scale to the enterprise. Technical administration and support costs are better controlled when limited resources can focus on this shared set of technology.

Implications:

- Technology platforms must be identified and documented, and analysis need 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.
- We are not freezing our technology baseline. We welcome technology advances and will change the technology architecture when compatibility with the current infrastructure, improvement in operational efficiency or a required capability has been demonstrated.

Principle 24: Seamless Integration

Statement:

Software and hardware should conform to defined standards that promote the seamless integration of data, applications and technology.

Rationale:

Standards help ensure consistency, which reduces the complexity of managing systems, improves user satisfaction and protects the existing information system investments. This maximizes return on investment and reduces costs.

Adhering to integration standards allows for support from multiple suppliers, reducing the cost associated with vendor lock-in.

Implications:

- Integration standards and industry standards will be followed unless there is a compelling business reason to implement a non-standard solution.
- A process for setting standards, reviewing and revising them periodically and granting exceptions must be established.
- The existing information system platforms must be identified and documented, and decisions need to be made about a process for convergence toward the newly defined standard.

Appendix A: Applying the principles – Examples

The scenarios below are purely hypothetical and do not reflect the prioritization that the initiative may receive. The questions and answers are examples designed to help the reader understand how the principles can help evaluate an initiative to ensure it aligns with the enterprise architecture.

The questions below are challenging and ensure proper consideration has been given to all aspects of information system initiatives. Depending on where you are in the development of an initiative you may not be able to answer the question in a linear fashion, but each principle needs to be assessed at some point.

Scenario 1: Alumni and Research Mapping

Advancement Communications and Engagement (ACE) has two mapping initiatives they would like to pursue.

The first initiative would allow alumni to reconnect with former classmates by sharing their location information and personal information on a map which can be accessed from the ACE website. The current ACE website supports only textual information sharing.

The second initiative is to promote outreach and engagement by visually showing outreach and engagement research activity on a map.

Application of Principles

Principle	Impact
Principled Decision Making	Are there any other considerations influencing the direction of this initiative? If so, what are they? *Yes, these initiatives were identified as some of the highest value activities on the ACE backlog.*
Maximize Value to the University	• What are the anticipated benefits? • What is the life expectancy of this initiative? • How will you determine if this initiative is successful? • How will you determine if this initiative is unsuccessful and needs to be stopped? • What is the anticipated total lifecycle costs to support this initiative? • What is the exit strategy and cost if this initiative doesn't realize the anticipated value? *It is anticipated that alumni interactions with others that have a shared background, and awareness of university initiatives and events in their area will result in increased support for the university.* *The existing service has been in place for several years but has very low usage. One of the goals of changing the service is to increase participation. If there is no increase in participation the service will be re-envisioned and the data converted or destroyed.*

Maintain Transparency in Information System Decision Making	Confirm which organizational unit(s) are affected by this initiative or change. This information will help determine the target governance committee. Who - aside from the original customer - might benefit from using this system? *At this point, it is not anticipated that any other unit will have a similar need.*

Plan for Continued Operations	• What instrumentation is delivered with the service that allows health, performance or utilization to be monitored?
	• What are the up-time requirements of the service?
	• What are the consequence of this service being offline?
	• Are there alternative modes of operation?
	• Does the service require redundancy?
	• Does this service rely on any other service or sub- service to be operational?
	• In a disaster scenario:
	  ○ How much data loss is tolerable?
	  ○ Is there a target recovery time?
	• What is the plan for addressing critical security patches, updates and renewals for this system? Do these patches happen automatically on a regular schedule or is someone responsible for watching for and applying these patches?
	• How will the system be scanned for vulnerabilities?
	
	The system isn't critical to our operations and we do not anticipate a need to develop an alternate mode of operation. Downtimes of a few days are tolerable as long as there is some indication that the service is temporarily offline.
	
	With regard to patching and vulnerability scanning of operating systems, the plan is to leverage internal platform services to host this system. This is addressed as part of their service offering. However, we will need to develop a process to handle lifecycle management and watch for critical fixes.

Minimize Duplication	• Is the desired functionality part of the future roadmap in a core or enterprise system?
	  ○ If so, is the current timeline acceptable?
	  ○ If the current timeline isn't acceptable, can the timelines be changed or a stop-gap solution be put in place?

	• If the desired functionality is not part of a future roadmap and there isn't an existing system that may support this initiative, is this a common need across campus? *There isn't a system that specifically provides this functionality but there are a number of services like mapping (GIS) that exist.*
Maintain Legal and Regulatory Compliance	• Are there any accreditation, regulatory or legal requirements associated with this system, the business processes or data? • Is the information in this system considered part of the core university business records? • Does this system store personal information, health data, credit card data or other sensitive information? *The system would collect personal information, but it is an optional service where the alumni and researchers are voluntarily supplying information to be discovered.* *If the service was wildly successful, this system could become a system or authority for alumni location information.*
Risk-Based Approach to Security	• How and by whom is the data collected, modified or disposed of? • What are the threats to this system or the information contained within it and what are the safeguards? • What data safeguards will control or limit access by individuals, support staff and administrators? *Alumni and researchers would be providing the information themselves, but modifying and deleting the data should be protected or at least limited to the individual that supplied it or a support staff member.* *The information is freely available to view online but it would be detrimental for the service and the university if an unauthorized person modified the data and added undesirable content. We need to control who can add, modify or delete the information and we will need to monitor content just in case.*
Information Systems Responsibility	• Who is the executive sponsor (AVP or Dean) accountable for this initiative? • Who is the business owner? • Who is the technical manager and owner of this initiative? • Has information about the initiative or system been recorded in the central application catalogue?

	The information will be recorded in the application catalogue. The executive sponsor is the AVP Communications. The director of communication and outreach is the line of business owner. The Manager, ICT Academic and Web Services is the technical manager.
Continuous Improvement	• What is the expected size of the user base? How is this initiative anticipated to change over the next three to five years? • Do you have current or forecasted metrics? ○ If not, how do you determine if you are improving something? • What processes will be put in place to gather, evaluate and report metrics? *The current system has low utilization and slow growth with maybe a few hundred entries in total and a few thousand views per year, but we anticipate a growth rate of 1,500 new entries per year. We are planning initiatives that direct people to this system and will need to develop a way to measure conversion.*

Data is an Asset	• What data is this system authoritative for?
	  ○ Who will govern it?
	• What are the business user's data quality requirements?
	• Will the information be of high enough quality that it can potentially be shared?
	• Does this system need data from other sources?
	  ○ If so, what is the integration model?
	
	The system is authoritative for geo-location of those alumni and research initiatives that have opted in. ACE will govern the data but we don't anticipate the data will be complete enough or of high enough accuracy that it will be useful for any other purpose.

Data is a Shared Resource	• Is the data from this system valuable to other systems or units on campus? ○ Should it be collected in central systems? • What is the model for exposing the data? *Unless the initiative becomes wildly successful there is no anticipated use for the data outside the system.*
Common Vocabulary and Data Definitions	• Are there accessibility guidelines, sensitive label and business rules for this data? • Is the external systems data used by this system consistent with the allowable usage identified in the university 'glossary' of data?

	This system may use information from the authentication services to get the name of the person posting their location. *We are planning on telling alumni that the location data will not be used for any other purpose.*
Data is Easily Accessible	• What integration model or techniques will be used to share data with other units, business processes or systems? • Is there a process being developed to help data users understand the data in this system, the responsibilities associated with it and the limits of its use? *We aren't currently planning on sharing the data.*
Data Manager	• Who will be ensuring the quality of the data? • Are there processes to review and validate user data to ensure that it's not out-of-date? • What processes will correct unsatisfactory data? • How will the data quality be measured? *We will need to develop a process to keep the data current (up to date) and age out information that is no longer relevant.*
Convergence with the Enterprise Architecture	• What system, manual or electronic process is this replacing? ○ Is there a deprecation plan for those service(s)? *There is an online system that helps locate alumni in your area. This initiative is a re-envisioning of that system and will enhance or replace it.*
Enterprise Architecture also Applies to External IT Providers	• Will this system or parts of it use external SaaS, PaaS or IaaS? ○ If the system is externally provided, how is the service provider addressing the principles? *As part of the solution development process we will evaluate on and off premise mapping services and will review this document to help with selection of the technology.*
Technology Independence	• Does the application support interchangeable components? ○ Web browsers ○ Operating systems ○ Physical and virtual hardware ○ Network components

	○ Cameras ○ Projectors ○ Directories *The system will need to support multiple browsers and mobile platforms. We will need to monitor the others.*
Ease-of-Use	• How does the look and feel compare to other university systems? • Will the application run on multiple devices, including mobile? *The site currently doesn't use the centrally supported visual identity templates but the visual styling and feel of the site is relatively consistent with other university sites.*
Component Simplicity and Reusability	• What business processes, data or parts of the information system are of general use or could be leveraged as a general purpose component? • Is this information system capable of leveraging existing infrastructure? *The authentication services will be leveraged to facilitate access to the system, but others are less clear.*
Reusable Interfaces	• Are interfaces being design for consumption by other systems? *Not applicable for this system. See data sharing above.*
Requirement Based Change	• Is there an established business need for this system? *Yes, see "Maximize Value to the University"*
Responsive Change Management	• Is it possible to deliver parts of the system immediately while other parts are being developed so the organizational unit can start to benefit immediately? *Yes, we could start by mapping alumni information and engagement research projects we already have permission to display then we could start getting feedback from potential clients while we improve data collection processes.*
Control Technical Diversity	• Are any new technologies, libraries or services being introduced to the university eco-system as a result of this initiative? ○ If so, are there barriers to them becoming the standard? *The goal will be to leverage existing technology standards and platforms and build on them where required.*

Seamless Integration	• How will this service be discovered? • How do users transition in and out of the service from other university services? *The service will be discovered both through the alumni pages within the main U of S website but also within PAWS as part of the alumni services area in PAWS.* *When navigating from PAWS some information may be pre-populated.*

Outcome

The recommendation for this initiative is a point solution to address mapping current information and data collection, a brief roadmap to aid in lifecycle management and monitoring for growth. Eventually with enough growth this initiative could becoming a shareable source of geolocation data for alumni.
Existing in-house tools and infrastructure should be leveraged where possible and the solution should be implemented in a way that strives to reduce the operational cost of support. Linkage to other systems on campus should be explored to improve discoverability.

Scenario 2: College Student Admissions System Renewal

In this scenario, a college identifies that it requires a new system for supporting the student admissions processes. The college has historically managed the processes manually using spreadsheets and online forms that result in emails to college administrative staff. However, this process is slow and error-prone and the volume of new applications now justifies a more robust system.
A Software as a Service (SaaS) vendor gave a presentation of their systems to the college and it looks very attractive.

Application of Principles

Principle	Impact
Principled Decision Making	Are there any other considerations influencing the direction of this initiative? If so, what are they? *No considerations aside from the principles.*
Maximize Value to the University	• What are the anticipated benefits? • What is the life expectancy of this initiative? • How will you determine if this initiative is successful? • How will you determine if this initiative is unsuccessful and needs to be stopped? • What is the anticipated total lifecycle costs to support this initiative?

	• What is the exit strategy and cost if this initiative doesn't realize the anticipated value? *The anticipated benefit includes a more robust process that reduces the reliance on administrative support staff to compile and process the applications.* *This systems is expected to last for the next 20 to 30 years.* *If successful, the overall time to process applications will be reduced by 20% and will have 30% fewer errors. It will be unsuccessful if it is cumbersome and negatively impacts the number of applications.* *The SaaS offering has a per user fee schedule of $20 per application received. Last year, the college received 2,000 applications. There was also a slight increase in recruitment activity which should increase applicants by 10%. So, the anticipated total cost is $40,000 to $50,000 for the year.* *It is unclear what the cost will be to get our data back from the vendor.*
Maintain Transparency in Information System Decision Making	Confirm which organizational unit(s) are affected by this initiative or change. This information will help determine the target governance committee. Who - aside from the original customer - might benefit from using this system? *All colleges on campus need some form of admissions processes and there is a central admissions system that doesn't address all of the requirements we have for admissions, and we are aware that some other colleges have their own admissions systems.* *We know whatever we do will need to integrate with the central student information system.*

Plan for Continued Operations	• What instrumentation is delivered with the service that allows health, performance or utilization to be monitored?
	• What are the up-time requirements of the service?
	• What are the consequence of this service being offline?
	• Are there alternative modes of operation?
	• Does the service require redundancy?
	• Does this service rely on any other service or sub- service to be operational?
	• In a disaster scenario:
	  ○ How much data loss is tolerable?
	  ○ Is there a target recovery time?

	• What is the plan for addressing critical security patches, updates and renewals for this system? Do these patches happen automatically on a regular schedule or is someone responsible for watching for and applying these patches? • How will the system be scanned for vulnerabilities? *Some of the detailed information requested here we don't have yet as we have only been assessing whether or not the system meets our requirements, but here is what we know.* *The vendor we looked at has reports about usage and performance.* *We accept applications at almost any time during the year so the system should be up 24 hours-a-day, 7 days-a-week.* *It would be unacceptable to lose any data and we need to ensure that this requirement is part of any service level agreement. The vendors service level agreement will need specific information about recovery times, loss of data, vulnerability scanning and how patching is addressed.*

Minimize Duplication	• Is the desired functionality part of the future roadmap in a core or enterprise system?
	  ○ If so, is the current timeline acceptable?
	  ○ If the current timeline isn't acceptable, can the timelines be changed or a stop-gap solution be put in place?
	• If the desired functionality is not part of a future roadmap and there isn't an existing system that may support this initiative, is this a common need across campus?
	
	The current student information system (SiRIUS) is only an 80-85% fit with the requirements, without customization. It is possible that the missing functionality is on a future roadmap.

Maintain Legal and Regulatory Compliance	• Are there any accreditation, regulatory or legal requirements associated with this system, the business processes or data? • Is the information in this system considered part of the core university business records? • Does this system store personal information, health data, credit card data or other sensitive information? *The information in this system would be part of the core university record and it contains personal information but there are no accreditation processes linked to admissions in this college.*

Risk-Based Approach to Security	• How and by whom is the data collected, modified or disposed of? • What are the threats to this system or the information contained within it and what are the safeguards? • What data safeguards will control or limit access by individuals, support staff and administrators? • Is the data center for this system in Saskatchewan or Canada? *Students who supply their application information to the system and administrative staff with the appropriate credentials can access the information.* *The data centers are in the United States.* *At this point, we are unaware of a way we can link this system to the central systems or use NSIDs. Therefore, the administrator will create an account for all support staff directly on this system and will use the U of S email address and a random five character password when setting up the account.*
Information Systems Responsibility	• Who is the executive sponsor (AVP or Dean) accountable for this initiative? • Who is the business owner? • Who is the technical manager and owner of this initiative? • Has information about the initiative or system been recorded in the central application catalogue? *Dean of Fictional College*
Continuous Improvement	• What is the expected size of the user base? How is this initiative anticipated to change over the next three to five years? • Do you have current or forecasted metrics? ○ If not, how do you determine if you are improving something? • What processes will be put in place to gather, evaluate and report metrics? *There were about 2,000 applicants that year and there has been a 10% increase in applicants over the last two years. This is anticipated to continue for at least two more years.* *We really need to monitor this because if the applicant pool more than doubles we don't have reserve funding to cover a $100K bill.*
Data is an Asset	• What data is this system authoritative for? ○ Who will govern it? • What are the business user's data quality requirements?

	• Will the information be of high enough quality that it can potentially be shared? • Does this system need data from other sources? ○ If so, what is the integration model? *Applicant information for the college. The Vice-Provost Teaching and Learning is the data steward for this information but the college will be responsible to ensure it is correct and flows into the student information system once the application is accepted.*
Data is a Shared Resource	• Is the data from this system valuable to other systems or units on campus? ○ Should it be collected in central systems? • What is the model for exposing the data? *It will be valuable to other units and colleges if the student is accepted. It may also be valuable to the university to understand how recruitment activity in on area affects other colleges.*
Common Vocabulary and Data Definitions	• Are there accessibility guidelines, sensitive label and business rules for this data? • Is the external systems data used by this system consistent with the allowable usage identified in the university 'glossary' of data? *The vendor may be able to supply this.*
Data is Easily Accessible	• What integration model or techniques will be used to share data with other units, business processes or systems? • Is there a process being developed to help data users understand the data in this system, the responsibilities associated with it and the limits of its use? *The SaaS vendor gives printable reports and csv files that we can use to import into other systems.*
Data Manager	• Who will be ensuring the quality of the data? • Are there processes to review and validate user data to ensure that it's not out-of-date? • What processes will correct unsatisfactory data? • How will the data quality be measured? *The manager of admissions in the college will need to be responsible for the data quality. This will require them to train staff on what is appropriate and develop processes to identify bad data and correct it before it becomes part of central system data.*

Convergence with the Enterprise Architecture	• What system, manual or electronic process is this replacing? ○ Is there a deprecation plan for those service(s)? *This is replacing some manual admissions processes, and a web form that can be pulled down once the new system is in place.*
Enterprise Architecture also Applies to External IT Providers	• Will this system or parts of it use external SaaS, PaaS or IaaS? ○ If the system is externally provided, how is the service provider addressing the principles? *Yes, there is a strong desire to go with the SaaS vendors' product.*

Technology Independence	• Does the application support interchangeable components?
	  ○ Web browsers
	  ○ Operating systems
	  ○ Physical and virtual hardware
	  ○ Network components
	  ○ Cameras
	  ○ Projectors
	  ○ Directories
	
	You can only use Mozilla Firefox to access the site, other browsers don't work well and result in strange layout problems.

Ease-of-Use	• How does the look and feel compare to other university systems? • Will the application run on multiple devices, including mobile? *It does not resemble other U of S systems, though we can contract the vendor to do layout customizations. It will not run on mobile devices.*
Component Simplicity and Reusability	• What business processes, data or parts of the information system are of general use or could be leveraged as a general purpose component? • Is this information system capable of leveraging existing infrastructure? *No possibility of re-use*
Reusable Interfaces	• Are interfaces being design for consumption by other systems? *No interfaces available. The vendor suggests they will have something for future releases.*
Requirement Based Change	• Is there an established business need for this system?

	Yes. See the Maximize Value principle.
Responsive Change Management	• Is it possible to deliver parts of the system immediately while other parts are being developed so the organizational unit can start to benefit immediately? *No, it is a turnkey system.*
Control Technical Diversity	• Are any new technologies, libraries or services being introduced to the university eco-system as a result of this initiative? ○ If so, are there barriers to them becoming the standard? *No, this is completely self-contained.*
Seamless Integration	• How will this service be discovered? • How do users transition in and out of the service from other university services? *A discoverable link would be setup from the college website.*

Outcome

The enterprise architecture recommendation is to re-use the SiRIUS system given the level of fit. A secondary recommendation is to review the admissions processes and enhance SiRIUS to address any gaps that aren't cost prohibitive.

The college may not be satisfied with this recommendation and may request an architecture exception. If an exception were to be granted, alternate vendors should be sought out due to poor integration options with existing campus assets. Partnering with this vendor would result in both initial and long-term costs that go well beyond the cost per applicant model assumed.

Appendix B: Glossary

Term	Definition
ISSC	The Information Systems Steering Committee is an executive-level committee reporting to PCIP and University Council. Setting strategic objectives and establishing institutional criteria for prioritizing systems initiatives will be done by this committee. The ISSC is accountable for overarching information systems policies, strategies and stewardship. This committee provides stewardship for the information systems project portfolio and it ensures information systems decisions have a strategic fit, functional utility and balanced investment across the institution. The committee will also address benefits realization of implemented projects. Enterprise architecture standards are approved by this group.
Enterprise	A university-wide context encompassing all of its information and technology services, processes and infrastructure.
Architecture	The fundamental organization of a system embodied by its components, their relationship to each other and the environment and the principles governing its design and evolution.
Enterprise Architecture	A conceptual architectural blueprint that defines the structures and operations of an organization.
Information Technology (IT)	A general term that refers to anything related to computer technology. This may include the people, software, servers, networking and the Internet.
Information Systems (IS)	A general term that refers to anything related to computer technology. This may include the people, software, servers, networking and the Internet.
Organizational Units	A generic term used to refer to colleges and departments within the university.
Vendor Lock-in	The situation in which the university is dependent on a vendor for products or services and is unable to use other vendors without a substantial switching cost.
COTS	Commercial Off-The-Shelf. A software package sold by a vendor.