Architectural Principles

Version 1.0

Table of Contents

UCIT Architectural Principles

1 General Information

This document presents the University of Calgary's Information Technologies' Architectural Principles.

These principles apply to all services and solutions provided by Information Technologies (UCIT). All UCIT staff are responsible for aligning their behaviours and decisions with them.

Architectural principles are derived primarily from business drivers, but also may be influenced by organizational policies, existing architectures, strategic business decisions, and trends in information technology. They are expressed at a high level and do not define standards and technology choices.

2 Intent

These principles are intended to form a common "value system", resulting in consistency in the application of UCIT resources.

3 Ownership

The principles are owned by the University's Chief Information Officer (CIO). The IT Architecture Standards Committee (ITASC) will provide a focal point for input on recommended changes, and will be responsible for publishing changes.

4 Applying the Principles

System architects must be careful to strike the right balance between the application of these (or any) principles and the need to encourage creativity and entrepreneurial behavior in the pursuit of strategic goals and objectives. Therefore, the Architectural Principles listed here are guiding principles, rather than directive in nature. Good judgment must be applied in their application.

5 Architectural Objectives

Architectural principles and standards are designed to achieve certain objectives. These include:

5.1. Ensure the U of C gets optimum value from UCIT resources, by maximizing capability and useful life.

5.2. Ensure alignment with the University of Calgary's Foundation Plan.

5.3. Ensure customer satisfaction with UCIT services.

5.4. Ensure a common understanding of objectives and strategies among UCIT staff and our customers.

5.5. Recognize that there may be significant educational, research, and partnership value in the use of different technologies and solutions.

5.6. Avoid duplication of effort.

5.7. Reduce the ongoing needs for maintenance, reintegration and customization.

5.8. Reduce single points of staff and technical dependency.

5.9. Minimize the need for education and training, for both service providers and the customer.

5.10. Provide effective, appropriate, and proportionate information security.

5.11. Ensure effective risk management.

5.12. Ensure that critical UofC information systems continue to function in the event of a disaster or prolonged service interruption.

5.13. Ensure that the infrastructure supports, and is responsive to, the evolving service needs of the University.

5.14. Promote efficiency through reuse, integration, and interoperability.

5.15. Provide the flexibility to adapt to business change.

5.16. Enable predictable delivery of services and solutions (schedule, budget, quality).

5.17. Balance immediate needs with technological progress.

5.18. Ensure the capability to measure and cost individual services.

5.19. Maintain data integrity and avoid data duplication and redundancy.

6 Architectural Principles

6.1 General

These principles define elements that should be considered for most UCIT activities.

6.1.1 ITASC will actively maintain and communicate architectural plans and ensure that they are in alignment with the University's Foundation Plan.

6.1.2 The Total Cost of Ownership (TCO) versus the expected benefits is a key architectural design criterion.

6.1.3 UCIT will provide proactive architectural leadership to all stakeholders on campus.

6.1.4 Pre-defined services and solutions will be used in preference to tailored solutions where they meet business needs in a cost-effective way.

6.1.5 Solutions chosen will be based predominantly on proven and best-of-breed technologies, bearing in mind the need to fit with existing and future systems and processes.

6.1.6 Services and solutions will be adequately supported. When new services are introduced, expertise will be acquired, or developed, as needed.

6.1.7 Solutions should be designed and/or selected to be accessible to the target user population through the modes and interfaces most appropriate for their use.

6.1.8 Service delivery at the U of C will be based on a coordinated model. UCIT will work with distributed IT groups to optimize the placement of individual service offerings and associated assets.

6.1.9 Services will be designed to include the collection of metrics to facilitate the measurement of the TCO and user satisfaction.

6.1.10 The source of funding for implementation, ongoing operation, maintenance, and sustainment must be identified before embarking on any new systems initiatives.

6.2 Information Security

These principles represent the basic information security requirements for the UCIT computing environment.

6.2.1 Services and solutions will be developed, maintained, and operated in a manner consistent with UCIT and University security policy, and industry best practices.

6.2.2 Services and solutions will include appropriate disaster recovery plans.

6.2.3 Solutions will include appropriate and proportionate security controls, including logical and physical access control mechanisms.

6.2.4 Services and solutions will include appropriate information security audit and assessment mechanisms.

6.2.5 Solutions will include appropriate risk assessment mechanisms.

6.3 Infrastructure

These principles define our basic approach to the acquisition, creation and operation of our underlying computing, communications and application component infrastructure.

6.3.1 The components shared by multiple units/faculties, such as network, desktops, servers, classroom technologies and applications, will be considered “infrastructure” and will be optimized on Total Cost of Ownership.

6.3.2 Interoperability, scalability, modularity, reliability, availability, and serviceability are key infrastructure design characteristics for infrastructure.

6.3.3 Infrastructure should be designed for broad utility rather than to solve particular end-user needs.

6.3.4 Infrastructure will be designed for centralized operations, monitoring, statistics collection and support.

6.3.5 UCIT will consciously invest in, and implement, infrastructure and supporting services in anticipation of business need.

6.3.6 Infrastructure components should be duplicated as necessary to provide platforms for testing, quality assurance, and training.

6.4 Campus-Wide Solutions

These principles define our basic approach for acquiring, creating, structuring, and supporting “Campus-Wide Solutions”, defined as information technology systems, including both software and hardware, which have wide utility across campus.

6.4.1 Campus-Wide Solutions should be developed, where possible, using industry standard approaches and methods.

6.4.2 Delivery approaches and methodologies should evolve in conjunction with industry trends and technology based on the value provided to the University.

6.4.3 The rigor applied when developing Campus-Wide Solutions should be commensurate with the size, complexity, and risk of those solutions.

6.4.4 Campus-Wide Solutions should be designed using a component-based architectural approach.

6.4.5 Campus-Wide Solutions should use existing infrastructure wherever practical for such things as identity and access management, persistent data storage, application servers, messaging, job scheduling, backup, etc.

6.4.6 Assets associated with Campus-Wide Solutions (e.g. source code, configuration information) should be maintained in a central repository that supports versioning, checkin/checkout, automated builds, etc.

6.4.7 Campus-Wide Solutions should include repeatable testing methods to ensure correct operation after any changes are made.

6.5 Innovative Solutions

These principles define our basic approach for acquiring, creating, structuring, and supporting solutions where innovation is a key criterion.

6.5.1 Innovative solutions will be considered where they uniquely support key business and academic priorities.

6.5.2 Innovative solutions should leverage existing infrastructure where possible.

6.6 Service Management

These principles define how UCIT systems are exposed as services both within and outside of UCIT.

6.6.1 UCIT will adopt a services management framework and define its offerings as individual services within that framework.

6.6.2 Service levels will be managed: service level objectives will be set, communicated and monitored, and actions taken to ensure targets are met.

6.6.3 Decisions regarding service level requirements should be made by the unit/faculty sponsor; however, UCIT needs to provide information regarding the total costs associated with varying levels of service.

6.6.4 The service support processes will be designed to route all Tier I support requests through a common service point.

6.7 Information Management

The principles define our basic approach to the way that we wish to create, control and protect the information stored in the University's business systems.

6.7.1 Data stored in University business systems is "owned" by the University as a whole, except where other contractual agreements have been made. Reuse for other purposes (in a manner consistent with University information management policy) is encouraged.

6.7.2 The information services and systems at the university should be designed with the needs of a cross-functional set of users in mind.

6.7.3 Data collected should be complete and captured once as early on in the business process to minimize data administrative efforts to cleanse data and ensure that it can be aggregated, analysed and manipulated for decision making purposes.

6.7.4 Data quality is managed to meet the business need for which it is intended. Data should be sufficiently accurate for its intended purpose, representing clearly and in sufficient detail the business process which it represents.

6.7.5 UCIT will play a proactive role in maintaining electronic information quality by ensuring appropriate system designs, and by ensuring that supporting processes are created as a part of system design.

6.7.6 All data elements stored in University business systems must have an identified "steward", which is an organizational unit responsible to ensure that the data is maintained and managed appropriately.

6.7.7 Data entities commonly used across the University will have unique identifiers that are managed centrally. Precise definitions of these entities are to be maintained in a "data dictionary".

6.7.8 Systems should expose their data and functionality via documented API's (e.g. web services, message queues) rather than requiring direct database access.

6.7.9 University-created information should be obtained directly from the source system and/or an appropriately managed secondary repository, e.g., application data warehouse, business intelligence tools.

6.7.10 The need for collecting data to support business metrics should be considered when architecting systems.