

Context and Principles

The following statements are intended to represent the business and technology landscape for the next three to five years. Thus, these items must be considered when discussing the future state vision.

Future State Context:

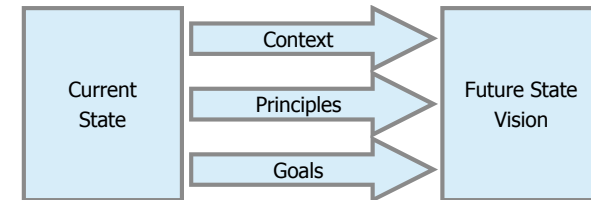
1. SAP will continue to be the primary ERP system; MIT may have other systems providing some ERP services
2. The MIT Data Warehouse will be the central repository for administrative data that is of interest to more than one DLC
3. Our user community will be based throughout the world, and will require 24x7 access to our systems; the definition of the MIT community will be amorphous, and will continue to evolve
4. There will be increased integration between MIT and other universities; there will be increased need for collaboration between members of MIT community and external community (e.g. other universities, research labs, etc.)
5. The MIT environment is heterogeneous
6. The MIT network will evolve to support needs of the enterprise; we may have many research networks, we will have an IPv6 network and we will need differentiated services to better support user needs

Goals

During the same discussions a number of goals were identified. These are listed below:

- Business rules and processes for accessing data will be well documented
- We will have a central repository (logical) for academic data
- We will eliminate "swivel chair" integration
- We will have a clear definition of what our community is but it may be complex with many parts

Future State | Context and Principles



Principles

Principles are intended to be simple statements of concepts that can be easily remembered, and used to guide the development of enterprise applications to evolve and improve the enterprise architecture. The statements below were agreed upon by the group and are intended to be used by application architects and developers to understand how they can contribute towards realizing MIT's enterprise architecture vision.

Security: applications should ensure data and access security

- Sensitive data must be protected in storage and in transit
- People should have single identity to all enterprise applications (single sign-on)
- Usernames should be consistent across applications

Ownership: clear and explicit ownership of enterprise data

- All enterprise level data entities should have a single identified system of record
- Systems should fulfill their custodial obligations for data they are the system of record for

Leverage assets: leverage existing services and capabilities

- Leverage capabilities in our existing investments where appropriate (SAP, Data warehouse, roles, etc.)

Accessibility: be aware of needs of all users (location & disabilities)

- Enterprise applications should be accessible from anywhere
- Enterprise applications should support accessibility standards

Real-time: Minimize latency of data updates

- Minimize latency of data updates

Standards: promote consistency using standards

- All new enterprise applications should adhere to recommended technical standards
- Use of open source tools and specifications

