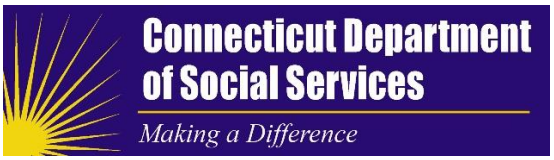

Enterprise Architecture: Principles

Version v0.05

Enterprise Architecture

Principles

Contents

Enterprise Architecture

Principles

Revision History

Date	Version	Author(s)	Notes
9/10/2018	0.03	Roger Bamford	Initial Draft
9/18/2018	0.04	Mike Montgomery	Format to CT DSS Document Style
11/15/18	0.05	Roger Bamford	Updates to Document

Enterprise Architecture

Principles

Introduction

This document details the Architecture Principles derived from the Open Group's TOGAF framework, MITA, FEAF, and from other government architecture frameworks available for use by the Department of Social Services, State of Connecticut. The purpose of this document is to define the IT Architecture Principles covering the five domains, Business, Data, Application, Technology and Security. This document contains the master list of the architectural principles.

IT architectural principles capture the high-level enterprise architecture strategy and guide the Information Technology Standards process. Principles provide high-level guidance to DSS initiatives to enhance productivity, ensure effective and efficient use of information technology. This document and the principles defined may be subject to adjustments as the enterprise refocuses its objectives.

Architectural Principles

Overview

An IT Architectural Principle is a high-level definition of the fundamental values to guide Business Information and Technology (IT) decision-making activities. They provide a foundation for both business and IT architectures, standards and help define the enterprise. Each EA Principle should focus on business goals and key architecture applications.

The Enterprise Architecture Principles document is owned by the Department of Social Services, Enterprise Architecture group and will be reviewed annually by the Architecture Governance Board. This document will be modified as needed or at each annual review.

It is important that all relevant architectural principles be considered when implementing or modifying existing systems and/or architectures.

Format

Each principle is enumerated with a rationale and impact statement, and will follow the format below.

ID	**<Principle ID>**
Name	**<Principle>**
Statement	The Statement communicates the fundamental architectural rule in sufficient detail to be clearly understood.
Rationale	The Rationale gives the strategic and business benefits of adhering to the principle.
Impact	The Impact statement communicates the cost, both for the business and IT, for implementing the principle – in terms of resources, costs, and activities / tasks.

Business Principles

BP-001: Scope of Architectural Principles

ID	BP-001
Name	**Scope of Architectural Principles**
Statement	These architectural principles are applicable to the Department of Social Services (DSS) unless exempted.
Rationale	DSS can achieve the benefits and efficiencies of an Enterprise Architecture and provide a consistent and measurable level of quality IT services to the citizens of Connecticut, when abiding by these architectural principles.
Impact	DSS initiatives will be reviewed for compliance with the IT architectural principles as part of the Enterprise Architecture governance process.

BP-002: Maximize Benefits

ID	BP-002
Name	**Maximize Benefits**
Statement	IT decisions should provide maximum benefit to the DSS, the staff, and their customers.
Rationale	Decisions made from an enterprise perspective have greater long-term value than decisions made from an individual perspective.
Impact	Solution components and information will be available across boundaries.

BP-003: Business Continuity

ID	BP-003
Name	**Business Continuity**
Statement	DSS operations are maintained in spite of system interruptions.
Rationale	Business operations throughout DSS will be provided with the capability to continue their business functions regardless of external events. Implementation of this capability will be dependent upon a risk assessment or business need. Hardware failure, natural disasters, and data corruption should not be allowed to stop or disrupt activities.
Impact	Dependency on shared system applications dictates that the risks of business interruption must be established in advance and managed. Management includes, periodic reviews, testing for vulnerabilities and exposure, or designing mission-critical services to ensure business continuity through redundant or alternative capabilities. Recoverability, redundancy, and maintainability should be addressed in the design phase of every project.

BP-004: Common Use Solutions

ID	BP-004
Name	**Common Use Solutions**
Statement	Development of solutions used across DSS is preferred. Development of similar solutions that are only provided to a limited audience are to be handled by exception.
Rationale	Duplicate capability is expensive and does not promote standardization or simplification.
Impact	Expenditures of scarce resources to develop essentially the same capability in marginally different ways will be reduced.

BP-005: Buy vs. Build

ID	BP-005
Name	**Build vs. Buy**
Statement	DSS prefers to buy services and solutions where possible. In-house development should be reserved for solutions that are not available in the marketplace.
Rationale	Buy vs. Build allows DSS to focus resources on the core mission while still enabling innovation. Common Off-The-Shelf (COTS) solutions are cheaper, quicker, and easier to implement and maintain.
Impact	Departments within the Department of Social Services should be encouraged to select COTS solutions through the RFQ / RFP process when there is a good fit with business requirements, and is economically viable.

BP-006: Compliance with Law

ID	BP-006
Name	**Compliance with Law**
Statement	Information management processes comply with all relevant laws, policies, and regulations.
Rationale	Information management processes are required to abide by laws, policies, and regulations. However, this is not meant to preclude business process improvements.
Impact	DSS must be mindful to comply with laws, regulations, and external policies regarding the collection, retention, and management of information. Changes in the law and changes in regulations may drive changes in processes or solutions.

BP-007: Cloud vs. On-Premise

ID	BP-007
Name	**Cloud vs. On-Premise**
Statement	DSS preferred location should be cloud based where possible. Cloud based solutions provide additional advantages over that of on premise solutions.

ID	BP-007
Rationale	Cloud based solutions enables DSS to focus resources on our core mission while still enabling innovation. Cloud based solutions are cheaper, quicker, and easier to implement and maintain and offer capabilities unavailable with on premise solutions.
Impact	Departments within DSS should be encouraged to select Cloud based solutions through the RFQ / RFP process when there is a good fit with business requirements, and is economically viable.

Data Principles

DP-001 – Data is a Shared Asset

ID	DP-001
Name	**Data is a Shared Asset**
Statement	Data is a shared asset that has value and is to be managed accordingly. Users have access to the data necessary to perform their duties; therefore, data should be shared across functions and agencies unless restricted by law.
Rationale	Timely access to accurate data is essential to improving the quality and efficiency of decision-making. It is less costly to maintain timely, accurate data in a single application, and then share it, than it is to maintain duplicative data in multiple applications. Data is a valuable State resource; it has real, measurable value. In simple terms, the purpose of data is to aid decision-making. Accurate, timely data is critical to accurate, timely decisions. Shared data will result in improved decisions relying on fewer sources of more accurate and timely managed data for all of our decision-making. Electronically shared data will result in increased efficiency when existing data entities can be used, without re-keying, to create new entities. Data should be collected once and shared. Wide access to data leads to efficiency and effectiveness in decision-making, and affords timely response to information requests and service delivery. Information use requirements must be considered from a State perspective to allow access by a wide variety of users. As the degree of data sharing grows and business units rely upon common information, it becomes essential that only the Data Owner make decisions about the content of data.
Impact	Data owners must have the authority and means to manage the data for which they are accountable. Secure data transfer techniques should be used when transferring data between agencies where required. Part of the role of data owner, is to ensure data quality. 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.

DP-002 – Data Integrity

ID	DP-002
Name	**Data Integrity**

ID	DP-002
Statement	Authority to create and maintain the data will reside with those most knowledgeable about the data or those most able to control its accuracy. Since data can lose its integrity when it is entered multiple times, the data owner will have sole responsibility for data entry, which eliminates redundant human effort and data storage resources.
Rationale	Those with the most knowledge of the data will have the greatest ability to maintain it accurately. Data integrity is at its highest level when the central management of changes to data is done by an authoritative source of record. Data owners must be accountable for the effective and efficient management of data. The accuracy, currency and security of data are management concerns best handled by data owners
Impact	It is essential to identify the true source of the data in order that the data authority can be assigned. Information should be captured electronically once and immediately validated as close to the source as possible. Quality control measures should be implemented to ensure the integrity of the data.

DP-003 – Data Definitions and Common Vocabulary

ID	DP-003
Name	**Data Definitions and Common Vocabulary**
Statement	Data is defined consistently and the definitions are understandable and available to all users.
Rationale	It is important that data that will be used in the development of applications must have a common definition to enable 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.
Impact	Data Owners must establish the initial common vocabulary for the business. The definitions will be used and any ambiguities resulting from multiple definitions of data must give way to accepted definitions and understanding. Multiple data standardization initiatives need to be coordinated.

DP-004 – Data Security

ID	DP-004
Name	**Data Security**
Statement	Secure data practices are used to avoid the inappropriate disclosure of sensitive or personally identifiable information and prevent unauthorized access.
Rationale	Open sharing of information and the release of information must be balanced against the need to restrict the availability of sensitive information. Existing laws and regulations must be followed regarding the safeguarding and privacy of data, while permitting free and open access.

ID	DP-004
Impact	Data owners and /or functional users must determine whether the aggregation of data results in an increased classification level. We will need appropriate policy and procedures to handle this review and reclassification. Access to information based on a need-to-know policy will force regular reviews of the body of information. In order to adequately provide access to open information while maintaining secure information, security needs must be identified and developed at the data level, not the application level. Security must be designed into data elements from the beginning; it cannot be added later. Systems, data, and technologies must be protected from unauthorized access and manipulation. State information must be safeguarded against inadvertent or unauthorized alteration, sabotage, disaster, or disclosure.

DP-005 – Data Integration

ID	DP-005
Name	**Data Integration**
Statement	Integration approach (real-time, overnight batch, etc.) will be driven by business needs. Where appropriate, real-time integration is preferred over batch integration.
Rationale	Today's business depend heavily on data for analysis, raising the stakes for data integration. At the same time, the work of integrating data has become increasingly complex. Unstructured data, big data, agency data, end-user data, and external data all challenge the old models for data integration. Meeting modern data integration challenges calls for a data integration strategy and architecture.
Impact	There are multiple integration technologies to share data and with multiple access points and multiple data hierarchies. This makes it very hard to track relationships between consumers and providers of data and the various copies of data, and makes it very hard to manage or understand the impact of change. Integration design should be driven by business needs, and leverage industry standards when available. It is difficult to manage the resource load on the data sources with multiple clients and direct access to the data sources. This exposes the source data too openly and makes it hard to manage the resulting load on the provider systems. Multiple security models and security mechanisms are required to serve the multiple clients with their multiple access technologies. The quality of service and interaction style is dictated by clients' access technologies. This means that the provider has to be able to support each client's technology and security model, which in turn makes it very difficult to manage security holistically over all these models and technologies. There is an inconsistent mechanism for meta data sharing. With no central meta data repository the semantics of the data become inconsistent and new formats for what is semantically the same data are created and must be maintained.

DP-006 – Data Replication

D	DP-006
Name	**Data Replication**
Statement	Minimize the replication of data within operational applications by replicating only stable data when necessary and based on business requirements.
Rationale	Replication should not be used unless it is required for performance or decision support, or for disaster recovery or backup. A replication infrastructure is simpler to design for stable data. If replicated data is updated frequently (i.e., not stable), it is much more difficult to design and maintain a replication infrastructure. It is better to maintain only one version of data whenever possible, particularly for mission critical online Transaction processing (OLTP) systems. Replication may be appropriate when there are users in different locations needing similar data that does not need to be current 24 hours a day and a central source database is not a possible solution.
Impact	Acceptable lag times must be defined to determine replication schemes, schedules, and the product features needed. Replication requirements must be defined to determine if the replication tools are sufficient. Business requirements must be documented for any data transformation requirements and for any differences in replication requirements. Specific application requirements for data availability, recoverability, and freshness (near real time, 24 hours old, etc.) must be identified. It is easiest to manage data quality and integrity when replicated and distributed data is read only. Document the business needs for any non-identical replicated copies of data and any data transformation requirements. Determine if replication processing overhead on the source and target databases will affect the performance of the applications using either database.

Application Principles

AP-001 - Ease-of-Use

ID	AP-001
Name	**Ease-of-Use**
Statement	Applications are easy to use. The underlying technology is transparent to users, so they can concentrate on the tasks at hand.
Rationale	The more a user has to understand the underlying technology, the less productive that user is. Ease-of-use is a positive incentive for users of applications. It encourages users to work within the integrated information environment instead of developing isolated systems to accomplish the task. Training is kept to a minimum and the risk of using a system improperly is low.
Impact	Guidelines for user interfaces should not be constrained by narrow assumptions about user location, language, systems training, or physical capability. Factors such as linguistics, customer physical infirmities (visual acuity, ability to use keyboard/mouse), and proficiency in the use of technology have broad ramifications in determining the ease-of-use of an application.

AP-002 - Applications Expose Data

ID	AP-002
Name	**Applications Expose Data**
Statement	Applications shall provide industry standards-based mechanisms and formats to expose and export their data for public and internal consumption.
Rationale	Applications are used to create and manage data that drives and guides DSS. Sharing data from its source leads to efficiency and effectiveness in decision-making; affords timely response to information requests and service delivery; and keeps the public informed and engaged in Government. Leveraging standards to expose data will ensure greater accessibility.
Impact	The implication is that there is an education task to ensure that all agencies understand the relationships between the value of data, sharing of data, and accessibility to data. Applications implement and enforce DSS's definitions of data. Data managed and shared through applications provides meaningful information to DSS and their customers.

AP-003 - Self-Serve

ID	AP-003
Name	**Self-Serve**
Statement	Customers should be able to serve themselves and DSS should encourage the use of the self-service applications.
Rationale	Applying this principle will improve customer satisfaction, reduce administrative overhead, and potentially improve efficiency.
Impact	There is an implication to improve ease-of-use and minimize training needs; for example, businesses should be able to modify their contact details, etc., and be able to acquire licenses and permits online.

AP-004 – System/Application Reuse

ID	AP-004
Name	**System/Application Reuse**
Statement	Department of Social Services will reuse existing enterprise application services and components to support business requirements where the existing functionality meets all mandatory requirements.
Rationale	Reuse of existing services and components helps manage complexity; drives lower total cost of ownership, increases operational efficiency and prevents service sprawl. Reusable components represent opportunities to reduce IT development times and costs. Reusable components leverage investments in current systems. Modular components increase the systems' capacities to adapt to different evolution needs, because the change is isolated from affected modules.
Impact	Department of Social Services IT Technology Catalog must be kept up-to-date with accurate and relevant details for users to reference. The development of applications based on Service Oriented Architecture (SOA) must be promoted and facilitated. Excessively complex configurations of components, undue customized tuning, and hardware and software customization based on transient, local, or other conditions must all be avoided. Component Reuse consists of the following categories: • Business Function components, • Technical Services components, • Commercial off the Shelf (COTS) components, and Reusable Code.

Technology Principles

TP-001 – Changes are Planned

ID	TP-001
Name	**Changes are Planned**
Statement	Changes to the DSS environment are planned and communicated.
Rationale	Planning changes provides a greater guarantee of successful and stable implementation. When changes are planned and communicated, conflicts are avoided and appropriate resources are made available.
Impact	Working together to ensure that change is well managed. The implication is that there is an education task to ensure that everyone understands the relationships between the need for change, planning changes, and responsiveness of change management.

TP-002 – Interoperability

ID	TP-002
Name	**Interoperability**
Statement	Software, hardware, and management and development processes should conform to defined standards that promote interoperability for data, applications, and technology.
Rationale	Standards help ensure consistency, thus improving the ability to manage systems and improve user satisfaction, and protect existing IT investments, thus maximizing return on investment and reducing costs. Standards for interoperability additionally help ensure support from multiple vendors for their products, and facilitate supply chain integration.
Impact	Interoperability standards and industry standards will be followed unless there is a compelling business reason to implement a nonstandard solution. A process for setting standards, reviewing and revising them periodically, and granting exceptions must be established.

TP-003 – Resiliency and Availability

ID	TP-003
Name	**Resiliency and Availability**
Statement	All technology components including data center physical and virtual infrastructure are designed in such a way to avoid any single point of failure. A standardized,

ID	TP-003
	consolidated infrastructure is used which helps to minimize risk, maximize network, storage and compute availability and support business continuity.
Rationale	Resiliency and availability must be designed in at inception. Implementation of this capability will be dependent upon a risk assessment or business need for each system.
Impact	Resiliency and availability requirements should be identified at the time of design. Applications must be assessed for criticality and impact on the State mission, in order to determine what level of resiliency and availability is required.

TP-004 – Scalability and Modularity

ID	TP-004
Name	**Scalability and Modularity**
Statement	Application architectures should be scalable, flexible and modular to meet ongoing and dynamic business growth.
Rationale	Architectures should be able to support a variety of legacy and emerging systems and technologies.
Impact	Standard scalability design patterns for each architectural domain should be published and periodically updated.

TP-005 – Industry Standard Technology

ID	TP-005
Name	**Industry Standard Technology**
Statement	Proposed architectures and technologies must support industry standards, and avoid proprietary technologies and interfaces unless specifically required for specialized applications or business needs.
Rationale	Industry standard technology and interfaces will reduce development cost, integration costs, and the time required to implement new functionality.
Impact	Approved technology standards must be published and maintained in an IT Standards Catalog.

Security Principles

SP-001 – Security Design

ID	SP-001
Name	**Security Design**
Statement	System architectures should employ security measures to ensure integrity, confidentiality and availability of IT services and applications. Security needs to be designed into the architecture in a scalable and efficient manner. The security architecture design should follow a modular design where the overall technology infrastructure is divided into functional layers / modules.
Rationale	The layered / modular approach allows the architecture to address the security relationship between the various functional blocks of the infrastructure and, it permits designers to evaluate and implement security on a module-by-module basis, instead of attempting to complete the architecture in a single phase.
Impact	Comprehensive published security standards for each layer / module of the IT architecture is a pre-requisite for all security designs.

SP-002 – Regulatory Compliance

ID	SP-002
Name	**Regulatory Compliance**
Statement	All architectures and solutions must meet all relevant legal and regulatory requirements, departmental standards and policies (including audit requirements), and industry best practices.
Rationale	Not following legal and regulatory requirements will introduce risk to the State and may result in legal action.
Impact	All legal and regulatory requirements for all applications and data must be cataloged and managed, and appropriate security standards published for each.

Associated Templates and Forms

Approvals

Role	Name & Title	Signature	Date
	Joe Stanford DSS Chief Innovation Officer		