

Office of Information Technology

Enterprise IT Architecture Principles

Version 1.0

May 2015

Table of Contents

OFFICE OF INFORMATION TECHNOLOGY	1
ENTERPRISE IT ARCHITECTURE	1
PRINCIPLES	1
1. PURPOSE OF THIS DOCUMENT.....	4
2. ARCHITECTURAL PRINCIPLES OVERVIEW.....	5
2.1. ARCHITECTURAL PRINCIPLES FORMAT.....	5
3. BUSINESS PRINCIPLES	6
3.1. BP-001 - STATEWIDE SCOPE OF ARCHITECTURAL PRINCIPLES.....	6
3.2. BP-002 - MAXIMIZE BENEFIT TO THE STATE.....	6
3.3. BP-003 - BUSINESS CONTINUITY.....	7
3.4. BP-004 - COMMON USE SOLUTIONS	8
3.5. BP-005 - BUY VS. BUILD	8
3.6. BP-006 - LIMIT CUSTOMIZATION	9
3.7. BP-007 - COMPLIANCE WITH LAW.....	9
3.8. BP-008 - ENABLE PRODUCTIVITY	10
3.9. BP-009 - DELIVER INFORMATION AND SERVICES WHEN AND WHERE NEEDED.....	10
3.10. BP-010 - MEET BUSINESS REQUIREMENTS.....	11
4. DATA PRINCIPLES.....	12
4.1. DP-001 – DATA IS A STATE SHARED ASSET	12
4.2. DP-002 – DATA INTEGRITY.....	13
4.3. DP-003 – COMMON VOCABULARY AND DATA DEFINITIONS	14
4.4. DP-004 – DATA SECURITY.....	15
4.5. DP-005 – DATA INTEGRATION	16
4.6. DP-006 – DATA REPLICATION.....	17
5. APPLICATION PRINCIPLES.....	19
5.1. AP-001 – MOBILE FIRST.....	19
5.2. AP-002 - EASE-OF-USE.....	20
5.3. AP-003 - APPLICATIONS EXPOSE DATA	21
5.4. AP-004 - SELF-SERVE.....	21
5.5. AP-005 – STATE APPLICATION COMPONENT REUSE.....	22
6. TECHNOLOGY PRINCIPLES.....	23
6.1. TP-001 – REQUIREMENTS-BASED CHANGE	23
6.2. TP-002 – TECHNOLOGY-BASED CHANGE	24
6.3. TP-003 – CHANGES ARE PLANNED	25
6.4. TP-004 – RESPONSIVE CHANGE MANAGEMENT.....	25

6.5.	TP-005 – USE STATEWIDE TECHNOLOGY INFRASTRUCTURE.....	26
6.6.	TP-006 – INTEROPERABILITY	27
6.7.	TP-007 – RESILIENCY AND AVAILABILITY	28
6.8.	TP-008 – SCALABILITY AND MODULARITY.....	29
6.9.	TP-009 – INDUSTRY STANDARD TECHNOLOGY	29
7.	SECURITY PRINCIPLES.....	30
7.1.	SP-001 – SECURITY DESIGN	30
7.2.	SP-002 – REGULATORY COMPLIANCE.....	30

List of Tables

Table 1-	Document Revision History.....	4
Table 2 -	Architectural Principle Format.....	5

1. Purpose of this Document

This document details the Enterprise Information Technology (IT) Architecture Principles for the State of Ohio.

The purpose of this document is to define the IT Architecture Principles by Business, Data, Application, Technology and Security domains. This document contains a master list of all IT architectural principles.

The IT architectural principles in this document capture the high-level enterprise architecture strategy of the State of Ohio and guide the Information Technology Standards process. Alignment with these principles will be verified as part of the Strategy and Investment Management review.

Principles provide high-level guidance to State initiatives to enhance productivity and ensure effective and efficient use of information technology across the State.

The principles in this document were developed in conjunction with external consultants, and are derived from the Open Group’s TOGAF standard, and from other government architecture principles.

The Enterprise IT Architecture Principles document is owned by the Enterprise IT Architecture & Policy group and is reviewed by the Technology Board prior to submission to the State CIO for final approval. This document will be updated as needed or at least annually.

Table 1- Document Revision History

Version #	Revision Date:	Revised by:	Description of Changes
1.0	May 2015		Initial Draft

2. Architectural Principles Overview

An IT Architectural Principle is defined as an enduring rule that governs the architectural design attributes and direction of a system or an overall enterprise. Architectural principles ensure industry best practices, cost and operational efficiencies, and compliance with the State’s Statutes, Provisions, Administrative Rules and Governor’s Executive Orders and Directives including the following:

Ohio IT-Related Statues:

- [ORC 125.18](#) Office of information technology – duties of director - contracts
- [ORC 1306](#) Uniform Electronic Transactions Act
- [ORC 1347.01](#) Personal information systems definitions

State Agency-Specific Provisions:

- [ORC 1306.20](#) State agency provisions
- [ORC 1306.21](#) Rules for state agency use of electronic records or signatures
- [ORC 1306.23](#) Exemptions to public records laws

It is mandatory that all relevant architectural principles be considered when designing architectures.

2.1. Architectural Principles Format

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

Table 2 - Architectural Principle Format

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.

3. Business Principles

Following are the architectural principles within the Business architectural domain.

3.1. BP-001 - Statewide Scope of Architectural Principles

ID	BP-001
Name	Statewide Scope of Architectural Principles
Statement	Pursuant to Ohio IT Policy ITP-A.1, “Authority of the State Chief Information Officer to Establish Policy Regarding the Acquisition and Use of Computer and Telecommunications Products and Services,” these architectural principles are applicable to every organized body, office, or agency established by the laws of the state for the exercise of any function of state government except for those specifically exempted.
Rationale	The State can only achieve the benefits and efficiencies of an Enterprise Architecture and provide a consistent and measurable level of quality IT services to the citizens of Ohio, when all agencies abide by these architectural principles.
Impact	IT initiatives will be reviewed for compliance with the IT architectural principles as part of the Strategy and Investment Management review. A conflict with a principle will need to be resolved by changing the design of the initiative, or requesting an exception.

3.2. BP-002 - Maximize Benefit to the State

ID	BP-002
Name	Maximize Benefit to the State
Statement	Information management decisions are made to provide maximum benefit to the State as a whole.
Rationale	Decisions made from a statewide perspective have greater long-term value than decisions made from any particular agency perspective.

Impact	<p>Solution components and information will be shared across Agency boundaries.</p> <p>Information management initiatives will be conducted in accordance with the statewide plan.</p> <p>Agencies may have to concede their own preferences for the greater benefit of the entire state.</p>
--------	---

3.3. BP-003 - Business Continuity

ID	BP-003
Name	Business Continuity
Statement	State operations are maintained in spite of system interruptions.
Rationale	<p>Business operations throughout the State must 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 for each system. Hardware failure, natural disasters, and data corruption must not be allowed to disrupt or stop State activities.</p>
Impact	<p>This principle is closely related with BP-009 Deliver Information and Services When and Where Needed and TP-007 – Resiliency and Availability.</p> <p>Dependency on shared system applications mandates that the risks of business interruption must be established in advance and managed. Management includes, but is not limited to, periodic reviews, testing for vulnerability and exposure, or designing mission-critical services to ensure business function continuity through redundant or alternative capabilities.</p> <p>Recoverability, redundancy, and maintainability should be addressed at the time of design.</p> <p>Applications must be assessed for criticality and impact on the State mission, in order to determine what level of continuity is required and what corresponding recovery plan is necessary.</p>

3.4. BP-004 - Common Use Solutions

ID	BP-004
Name	Common Use Solutions
Statement	Development of solutions used across the State is preferred over the development of similar or duplicative solutions that are only provided to a particular agency.
Rationale	Duplicative capability is expensive and proliferates conflicting information.
Impact	This principle is closely related to: DP-001 Data is a State Shared Asset. Agencies will not be allowed to develop capabilities for their own use that are similar/duplicative of statewide capabilities. In this way, expenditures of scarce resources to develop essentially the same capability in marginally different ways will be reduced.

3.5. BP-005 - Buy vs. Build

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

3.6. BP-006 - Limit Customization

ID	BP-006
Name	Limit Customization
Statement	Leverage solutions that require little or no customization to meet the needs.
Rationale	Limiting customization decreases the risks that a solution will become unsupportable and controls the total cost of ownership.
Impact	Leverage solutions that require no customization to meet the needs. Customized solutions require more maintenance over time, have a higher risk of becoming unsupportable, and increase the life cycle management which overall increases total cost of ownership.

3.7. BP-007 - Compliance with Law

ID	BP-007
Name	Compliance with Law
Statement	State information management processes comply with all relevant laws, policies, and regulations.
Rationale	State information management processes are required to abide by laws, policies, and regulations. However, this is not meant to preclude business process improvements that lead to changes in policies and regulations.
Impact	<p>The State must be mindful to comply with laws, regulations, and external policies regarding the collection, retention, and management of information.</p> <p>Changes in the law and changes in regulations may drive changes in our processes or solutions.</p>

3.8. BP-008 - Enable Productivity

ID	BP-008
Name	Enable Productivity
Statement	Employees and agents of the State should have the tools they need to be productive.
Rationale	Applying this principle will improve the productivity of employees and agents of the State.
Impact	There is an implication to improve the efficiency and effectiveness of government and reduce costs.

3.9. BP-009 - Deliver Information and Services When and Where Needed

ID	BP-009
Name	Deliver Information and Services When and Where Needed
Statement	The architecture allows for the availability of information and services when and where needed.
Rationale	<p>The State is more effective, efficient, and responsive when:</p> <ul style="list-style-type: none"> • Agencies deliver services when and where they are needed or desired • Agencies address issues when and where they present themselves
Impact	<p>This principle is closely related with BP-003 Business Continuity and TP-007 – Resiliency and Availability.</p> <p>There is an implication to improve the efficiency and effectiveness of government and reduce costs in the long-term.</p> <p>There is an implication that enabling services to be available at anytime from anywhere may require significant upfront investment.</p>

3.10. BP-010 - Meet Business Requirements

ID	BP-010
Name	Meet Business Requirements
Statement	Solutions should be designed to meet business requirements, maximize value and productivity, and minimize rework and cost.
Rationale	Defined business requirements will enable a solution design that meets all requirements and aligns with enterprise architecture standards and principles.
Impact	Business owners must formally define in a business requirements document expected levels of service for functionality, usability, performance and availability.

4. Data Principles

Following are the architectural principles within the Data architectural domain.

4.1. DP-001 – Data is a State Shared Asset

ID	DP-001
Name	Data is a State Shared Asset
Statement	<p>Data is a State shared asset that has value to the State and is managed accordingly. Users have access to the data necessary to perform their duties; therefore, data is shared across State functions and agencies unless restricted by law.</p>
Rationale	<p>Timely access to accurate data is essential to improving the quality and efficiency of State 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.</p> <p>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. Data is the foundation of our decision-making, so we must also carefully manage data to ensure that we know where it is, can rely upon its accuracy, and can obtain it when and where we need it.</p> <p>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.</p> <p>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.</p> <p>As the degree of data sharing grows and business units rely upon common information, it becomes essential that only the Data Owner makes decisions about the content of data.</p>

Impact	<p>This principle is closely related to BP-004 Common Use Solutions.</p> <p>Data Sharing across State entities should be supported by data usage agreements that cover controls on data security, data access, data usage, data retention, and data destruction.</p> <p>Data owners must have the authority and means to manage the data for which they are accountable.</p> <p>Secure data transfer techniques should be used when transferring data between agencies where required.</p> <p>The role of data owner is critical because obsolete, incorrect, or inconsistent data could be passed to State personnel and adversely affect decisions across the State.</p> <p>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.</p>
--------	--

4.2. DP-002 – Data Integrity

ID	DP-002
Name	Data Integrity
Statement	<p>Authority to create and maintain the data will reside with those most knowledgeable about the data or those most able to control its accuracy.</p> <p>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.</p>
Rationale	<p>Those with the most knowledge of the data will have the greatest ability to maintain it accurately.</p>

	<p>Data integrity is at its highest level when the central management of changes to data is done by an authoritative source of record.</p> <p>Data owners must be accountable for the effective and efficient management of data.</p> <p>The accuracy, currency and security of data are management concerns best handled by data owners.</p>
Impact	<p>It is essential to identify the true source of the data in order that the data authority can be assigned.</p> <p>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.</p>

4.3. DP-003 – Common Vocabulary and Data Definitions

ID	DP-003
Name	Common Vocabulary and Data Definitions
Statement	Data is defined consistently throughout the State, 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 throughout the State 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	<p>Data Owners must establish the initial common vocabulary for the business. The definitions will be used uniformly throughout the State.</p> <p>Ambiguities resulting from multiple definitions of data must give way to accepted statewide definitions and understanding.</p> <p>Multiple data standardization initiatives need to be coordinated.</p>

4.4. 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	<p>Open sharing of information and the release of information via relevant legislation must be balanced against the need to restrict the availability of classified and sensitive information.</p> <p>Existing laws and regulations require the safeguarding and privacy of data, while permitting free and open access.</p>
Impact	<p>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 re-classification. Access to information based on a need-to-know policy will force regular reviews of the body of information.</p> <p>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.</p> <p>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.</p>

4.5. 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	<p>Today’s managers depend heavily on data 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.</p>
Impact	<p>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.</p> <p>Integration design should be driven by business needs, and leverage industry standards when available.</p> <p>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.</p> <p>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.</p> <p>There is an inconsistent mechanism for meta data sharing. With no central meta data repository the semantics of the data become</p>

	<p>inconsistent and new formats for what is semantically the same data are created and must be maintained.</p> <p>It is hard to track usage of the data and therefore hard to understand the impacts of change.</p> <p>There is inconsistent data quality because of the various formats and copies of the data. This makes it very hard to understand</p> <ul style="list-style-type: none"> • Who has latest copy? • Who's using the latest copy? • What's the correct value for data, now?
--	--

4.6. DP-006 – Data Replication

ID	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	<p>Replication should not be used unless it is required for performance or decision support, or for disaster recovery or backup.</p> <p>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.</p> <p>It is better to maintain only one version of data whenever possible, particularly for mission critical online Transaction processing (OLTP) systems.</p> <p>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.</p>
Impact	<p>Acceptable lag times must be defined to determine replication schemes, schedules, and the product features needed.</p> <p>Replication requirements must be defined to determine if the replication tools are sufficient.</p>

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.

Determine if network traffic required for replication can impact communication costs and performance.

5. Application Principles

Following are the architectural principles within the Application architectural domain.

5.1. AP-001 – Mobile First

ID	AP-001
Name	Mobile First
Statement	The State is adopting a MOBILE FIRST Strategy that applies to business applications, whether citizen, business or state employee facing.
Rationale	Mobile access has become an integral part of how we communicate, organize our lives and obtain support and services. As a result, citizens, businesses and state employees are using smart phones and tablets everywhere, impacting how they interact with the State on a daily basis. State agencies maintain a wealth of capabilities, systems and data that can positively influence the day-to-day lives of our constituents and employees. The State has a significant responsibility in delivering services to citizens and businesses in Ohio and delivering services in a manner they expect. IT and systems are an intrinsic part of how we do business and are a key enabler of providing State services to the mobile public.
Impact	<p>New applications or significant upgrades to existing applications should be designed for MOBILE FIRST when cost effective and appropriate.</p> <p>Make it easy to do business with the State by helping our customers find what they are looking for, completing forms or approvals, contacting the State for support - simply put - mobile applications make citizens' lives easier in seeking information, navigating services, applying for assistance, asking for help and getting updates on progress.</p> <p>Make it easier for the State to do business by helping state staff be more productive, providing higher levels of customer service, streamlining workflows and approvals, providing real time access to State data, and</p>

	<p>eliminating complexity through simpler mobile applications and interfaces.</p> <p>Agencies should actively seek to make existing websites mobile adaptive and reflexive by including mobile access requirements as a mandatory consideration in new applications and system upgrades and implementations. Adaptive websites automatically sense and adjust onscreen content to be readable and usable on mobile devices.</p>
--	---

5.2. AP-002 - Ease-of-Use

ID	AP-002
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. (State of Ohio IT Policies IT-06, IT-08, ITP-F.3, and ITP-F.35)
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 outside of the State's integrated information environment. 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.

5.3. AP-003 - Applications Expose Data

ID	AP-003
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 the State. 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	<p>This principle is closely-related to DP-001 Data is a State Shared Asset. 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.</p> <p>Applications implement and enforce the State's definitions of data. Data managed and shared through applications provides meaningful information to the State and its constituency.</p>

5.4. AP-004 - Self-Serve

ID	AP-004
Name	Self-Serve
Statement	Customers should be able to serve themselves and the State 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.

5.5. AP-005 – State Application Component Reuse

ID	AP-005
Name	State Application Component Reuse
Statement	The State will reuse existing enterprise application services and components to support business requirements where the existing functionality meets all mandatory requirements.
Rationale	<p>Reuse of existing services and components helps manage complexity; drives lower total cost of ownership, increases operational efficiency and prevents service sprawl.</p> <p>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.</p>
Impact	<p>The State of Ohio IT Services Catalog must be kept up-to-date with accurate and relevant details for users to reference.</p> <p>The development of applications based on Service Oriented Architecture (SOA) must be promoted and facilitated.</p> <p>Excessively complex configurations of components, undue customized tuning, and hardware and software customization based on transient, local, or other conditions must all be avoided.</p> <p>Component Reuse consists of the following categories:</p> <ul style="list-style-type: none"> • Business Function components, • Technical Services components, • Commercial off the Shelf (COTS) components, and • Reusable Code.

6. Technology Principles

Following are the architectural principles within the Technology architectural domain.

6.1. TP-001 – Requirements-Based Change

ID	TP-001
Name	Requirements-Based Change
Statement	Changes to applications and technology are in response to the business or legislative needs of the State.
Rationale	<p>This principle will foster an atmosphere where the information environment changes in response to the needs of the business, rather than having the business change in response to IT changes. This is to ensure that the purpose of the information support – the transaction of business – is the basis for any proposed change. Unintended effects on business due to IT changes will be minimized.</p> <ul style="list-style-type: none"> • A change in technology may provide an opportunity to improve the business process and, hence, change business needs. • A change in technology may provide an opportunity to improve security and, hence, change or improve an existing business need. • A change in technology may ensure the maintainability of a service supporting a business function and, hence, support an existing business need. <p>The only exception to this principle is technology driven change to support modernization of aging technology platforms. See TP-002 Technology-Based Change.</p>
Impact	This is one of four closely-related principles regarding change: TP-001 Requirements-Based Change; TP-002 Technology-Based Change, TP-003 Changes Are Planned; and TP-004 Responsive Change Management. These four principles work together to ensure that change is well-managed. The implication is that there is an education task to ensure that all agencies understand the relationships between the need for change, planning changes, and responsiveness of change management.

	<p>Changes in implementation will follow full examination of the proposed changes using the enterprise architecture.</p> <p>Change management processes will be developed or modified and implemented to conform to this principle.</p> <p>This principle may conflict with the Responsive Change Management principle. We must ensure the requirements documentation process does not hinder responsive change management to meet legitimate business needs. The purpose of this principle is to keep us focused on business, not technology needs – responsive change management is also a business need.</p>
--	---

6.2. TP-002 – Technology-Based Change

ID	TP-002
Name	Technology-Based Change
Statement	Changes to applications and technology are only in response to business needs of the State, except in the case of modernization of aging technology platforms, or research & development projects that are evaluating new technologies or approaches
Rationale	Modernization of an aging technology platform should ensure the maintainability of a service supporting a business function and, support conformance to IT enterprise standards.
Impact	<p>This is one of four closely-related principles regarding change: TP-001 Requirements-Based Change; TP-002 Technology-Based Change, TP-003 Changes Are Planned; and TP-004 Responsive Change Management. These four principles work together to ensure that change is well-managed. The implication is that there is an education task to ensure that all agencies understand the relationships between the need for change, planning changes, and responsiveness of change management.</p> <p>Changes in technology will follow full examination of the proposed changes using the enterprise architecture.</p>

6.3. TP-003 – Changes are Planned

ID	TP-003
Name	Changes are Planned
Statement	Changes to the State Information Technology 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	<p>This is one of four closely-related principles regarding change: TP-001 Requirements-Based Change; TP-002 Technology-Based Change, TP-003 Changes Are Planned; and TP-004 Responsive Change Management. These four principles work together to ensure that change is well-managed. The implication is that there is an education task to ensure that all agencies understand the relationships between the need for change, planning changes, and responsiveness of change management.</p> <p>We have to develop processes for managing and implementing change that provide assurance of success.</p> <p>Agencies will have to be involved in change management.</p> <p>IT will have to be aware of business plans that require changes to the State information environment.</p>

6.4. TP-004 – Responsive Change Management

ID	TP-004
Name	Responsive Change Management
Statement	Changes to the State Information Technology Environment are implemented in a timely manner.
Rationale	If agencies are to be expected to work within the statewide information environment, that information environment must be responsive to their needs.

Impact	<p>This is one of four closely-related principles regarding change: TP-001 Requirements-Based Change; TP-002 Technology-Based Change, TP-003 Changes Are Planned; and TP-004 Responsive Change Management. These four principles work together to ensure that change is well-managed. The implication is that there is an education task to ensure that all agencies understand the relationships between the need for change, planning changes, and responsiveness of change management.</p> <p>We have to develop processes for managing and implementing change that do not create delays.</p> <p>A “business expert” must facilitate explanation and implementation when an agency feels a need for change.</p> <p>If we are going to make changes, we must keep the architectures up-to-date.</p>
--------	--

6.5. TP-005 – Use Statewide Technology Infrastructure

ID	TP-005
Name	Use Statewide Technology Infrastructure
Statement	Use of the Statewide Technology Infrastructure allows the State to control technological diversity and to minimize the non-trivial cost of maintaining multiple different environments and locations.

<p>Rationale</p>	<p>There is a real, non-trivial cost of infrastructure required to support alternative technologies and environments.</p> <p>Limiting the number of supported components will simplify maintainability and reduce costs.</p> <p>The business advantages of minimum technical diversity include:</p> <ul style="list-style-type: none"> • Standard packaging of components; • Predictable implementation impact; • Increased flexibility to accommodate technological advancements. <p>Common technology across the State brings the benefits of economies-of-scale to the State.</p> <p>Technical administration and support costs are better controlled when limited resources can focus on this shared set of technology.</p>
<p>Impact</p>	<p>Policies, standards, and procedures that govern acquisition of technology must be tied directly to this principle.</p> <p>Technology choices will be constrained by the choices available within the Statewide Technology Infrastructure and roadmap. Procedures for augmenting the acceptable technology set to meet evolving requirements will have to be developed and put in place.</p> <p>We are not freezing our technology baseline. We welcome technology advances and will change the Statewide Technology Infrastructure and roadmap when compatibility with the current infrastructure, improvement in operational efficiency, or a required capability has been demonstrated.</p>

6.6. TP-006 – Interoperability

<p>ID</p>	<p>TP-006</p>
<p>Name</p>	<p>Interoperability</p>
<p>Statement</p>	<p>Software, hardware, and management and development processes should conform to defined standards that promote interoperability for data, applications, and technology.</p>

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	<p>Interoperability standards and industry standards will be followed unless there is a compelling business reason to implement a non-standard solution.</p> <p>A process for setting standards, reviewing and revising them periodically, and granting exceptions must be established.</p>

6.7. TP-007 – Resiliency and Availability

ID	TP-007
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, consolidated infrastructure is used which helps to minimize risk, maximize network, storage and compute availability and support business continuity.
Rationale	The State’s technology investment supports mission-critical citizen services, and 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	<p>This principle is closely related with BP-003 – Business Continuity and BP-009 Deliver Information and Services When and Where Needed.</p> <p>Resiliency and availability requirements should be identified at the time of design.</p> <p>Applications must be assessed for criticality and impact on the State mission, in order to determine what level of resiliency and availability is required.</p>

6.8. TP-008 – Scalability and Modularity

ID	TP-008
Name	Scalability and Modularity
Statement	State and agency application architectures should be scalable, flexible and modular to meet ongoing and dynamic business growth.
Rationale	State and agency architectures 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.

6.9. TP-009 – Industry Standard Technology

ID	TP-009
Name	Industry Standard Technology
Statement	State and agency 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	State approved technology standards must be published and maintained in the statewide IT Standards Catalog.

7. Security Principles

Following are the architectural principles within the Security architectural domain.

7.1. SP-001 – Security Design

ID	SP-001
Name	Security Design
Statement	State and agency 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.

7.2. SP-002 – Regulatory Compliance

ID	SP-002
Name	Regulatory Compliance
Statement	All state and agency architectures and solutions must meet all relevant legal and regulatory requirements, State 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.