General Architecture Principles

It is understood that formal Policies, Standards, Procedures, etc. will never exhaustively encompass every single aspect of Maine State Information Technology (I.T.). Yet, each I.T. stakeholder is faced with critical decisions as an integral part of their everyday work. Such everyday decisions frequently have lasting consequences in terms of costs and benefits of I.T. However, it is difficult to anchor everyday I.T. decisions in the absence of a general framework of principles. Therefore, a set of general architecture principles have been developed to aid in everyday decision-making. These principles are based upon the Federal Enterprise Architecture Framework Version 2.0 (FEAF-II)\(^1\).

1. The State is a single, unified enterprise.
2. Information is a statewide asset.
3. Security and Privacy are core missions.
5. Cloud First.
6. First reuse; then buy; then build.
7. Choose new products carefully.

Rationale

1. *The State is a single, unified enterprise.* A single I.T. enterprise with shared products and policies lowers costs and improves service. Further, any attempt at optimization is more likely to be fruitful when it targets the State as a whole rather than a single agency or program. Economies of scale not only extract deeper discounts from vendors but also facilitate interoperability and cross-training, thereby lowering costs and improving supportability. For example, it is simply impossible to actualize robust Cyber Security or Disaster Recovery unless the State is treated as a single, unified enterprise. The Maine State Executive Branch consolidated its I.T. operations back in 2005, and it continues to reap the rewards in terms of better service and lower total cost of ownership. It remains in the best interests of all parties to continue this trend and explore greater opportunities for collaboration and standardization across the State.

2. *Information is a statewide asset.* Quality information is critical to effective government decision-making and fulfilling the government's obligation to its citizenry. To achieve this goal, the desired state is to have authoritative well defined sources of data elements across all IT platforms regardless of department/agency. Currently, common data elements are dispersed across multiple information systems, with disparate formats, contexts, and meanings. Authoritative sources of particular data elements are often not well-documented, and stewardship is not codified. Such a state of affairs impedes statewide information flow, leading to poor decision-making. Lacking effective data/information standards, agencies and programs are currently left to creating ad-hoc solutions, leading directly to the fragmentation of the State’s information assets, compromised accuracy and integrity of its reports, increased operational

costs, and weaker security. A concerted, business-side effort must be launched to standardize data elements, codify systems of record and stewardship, and move toward standards-based data-exchange formats (such as XML and/or JSON).

3. **Security and Privacy are core missions.** The citizens of Maine trust their government with an immense cache of personally identifiable information. It is absolutely essential for the State to reciprocate that trust with the best possible protection of that cache. Therefore, Security and Privacy of information is the cornerstone of all government operations. Citizens explicitly expect their government to apply security and privacy consistently and monitor compliance. Security controls must be clearly defined so that costs and risks may be balanced appropriately. The State should implement security and privacy practices at all levels of government to ensure the confidentiality, integrity, and availability of its information assets. The State must do everything in its power to protect its information assets from unauthorized or accidental use, disclosure, disruption, modification, or destruction.

4. **Centralize Authentication; Federate Authorization.** Authentication of user and device identities need to be centralized to improve service, enable single credential and/or single sign-on, and reduce application development and support costs. Centralization of authentication permits appropriate management and security controls to be applied universally. Make applications & appliances consume authentication from external directories. To that end, Microsoft Active Directory (A.D.) remains the State's standard directory product. Any and all I.T. products within the state must be fully A.D.-aware.

Individual applications and appliances are free to maintain their own dedicated authorization (roles & privileges) modules. However, wherever two or more applications or appliances must share authorizations, they should consider federating such authorizations to a neutral repository, with the system of record granted complete control to manage such authorizations.

5. **Cloud First.** By default, there exists a strong preference toward Commercial Public Cloud for hosting all new assets, including replacement of existing assets. Within Commercial Public Cloud, the order of preference is:

1. Software-as-a-Service
2. Platform-as-a-Service
3. Infrastructure-as-a-Service

It is understood that there do exist legitimate reasons for the occasional on-premises hosting; They include statutory constraints, bandwidth constraints, lack of appropriate Commercial Public Cloud offering, etc. However, Commercial Public Software-as-a-Service remains the preferred selection.

Where Software-as-a-Service is not readily available, the preference is for the
asset provider to hire a Platform-as-a-Service or Infrastructure-as-a-Service intermediary who effectively packages the original offering in order to expose it as Software-as-a-Service. By utilizing this approach, we have a single entity responsible for the entire solution (the original asset provider and their hired intermediary) as opposed to two separate entities each responsible for a portion of the solution.

6. **First reuse; then buy; then build.** Clearly, the best value to be extracted from sunken investments is to reuse them to the maximum extent possible. Unfortunately, due to the pace of innovation in I.T., as well as the aggressive nature of marketing, the technology sector is more susceptible to hype than other sectors. Nevertheless, the State needs to summon the discipline to stick with the products that it already owns, as long as they continue to deliver an acceptable level of performance to its customers, and as long as vendors continue to support said products. Specifically, the State should consider exploiting additional capabilities of products it already owns that are still supported by their vendors, even when they may not be the best-of-breed in a particular niche.

If it is determined without a doubt that an existing I.T. asset cannot meet current requirements, then the State should explore an off-the-shelf product that comes the closest to satisfying such unmet requirements. It is likely that the State will need to modify its workflows and business processes in order to utilize an off-the-shelf product, but that is still preferable to creating a custom product exclusively for its requirements.

Only if it is ascertained that there really does not exist any off-the-shelf product that comes even close to meeting its requirements should the State explore the option of building a custom product. But this better be the option of the very last resort. All else being equal, the lifetime total cost of ownership for a custom product usually exceeds that of an off-the-shelf product.

7. **Choose new products carefully.** In the past, individual arms of the State have acquired products on their own without much coordination with one other. The accumulative effect of that is the current reality, a smorgasbord of competing products. This has some obvious disadvantages: lack of interoperability, lack of adequate support, lack of depth of coverage, lack of economies of scale, etc. In order to ensure greater success of I.T. in the State, it is critical to limit the buffet of technology options. This will enhance interoperability for there will be fewer moving parts to interface with. This will increase the level and depth of support for there will be a higher headcount per technology option, directly leading to higher in-house expertise. This will increase economy of scale for there will be a higher market share per technology option, directly leading to increased pressure on vendors to provide deeper discounts, dedicated training, etc. Taken together, limiting the buffet of technology options promises to reduce I.T. costs and improve service.
The marketplace continues to explode with new products at a rapid pace. Clearly, no single entity, least of all the State, can afford to sample them all indiscriminately. That said, the State also cannot allow itself to fall too far behind the technology curve, lest it deprives itself of viable superior options. Therefore, it needs to chart a prudent middle course that can both filter out the hype, and yet discern lasting trends that have the potential to deliver higher returns. The product/technology selection criterion is as follows, in descending order of importance:

1. *Ability to Meet Requirements*
2. *Customer Value (Return on Investment)*
3. *Installed Base within the State*
4. *Supportability*
5. *Scalability*
6. *Sustainability (Viability)*
7. *General Excellence & Market Position*
8. *Alignment with Long-term Architecture*

Ability to Meet Requirements should command the highest weight. Customer Value (Return on Investment) cost considerations should be holistic, not just the one-time cost of acquisition, but a best guesstimate of the lifetime total cost of ownership. If a product/technology has a large installed base within the State and the State is already comfortable supporting it, it makes sense to continue with that product/technology and negotiate a deeper volume discount from the vendor. Scalability and Sustainability (Viability) are important from an enterprise perspective. There exist I.T. products that were originally acquired by individual agencies, which may have been adequate for meeting the requirements of those individual agencies, but do not scale, and therefore, cannot be sustained on an enterprise basis. It goes without saying that it is in the best interests of the State to bank on products that command positions of excellence in the marketplace. Finally, it is also in the best interests of the State to select products that are in alignment with its long-term architecture vision.

Latest Revision Date: December 8, 2015