General Architecture Principles

It is understood that formal Policies, Standards, Procedures, etc. can 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* has been developed to aid in that everyday decision-making.

1. The State is a single, unified enterprise
2. Agencies are the caretakes of the data that they transact
3. Security & Privacy are foundational to everything else
4. Accessibility is a core mission
5. Centralize Authentication; Federate Authorization
6. First reuse; Then buy; Then build
7. Choose new products carefully to support modernization
8. Be Cloud-Smart

Each of the above principles is elaborated below.

1. *The State is a single, unified enterprise.* A single I.T. enterprise with shared products and policies lowers cost, 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 discount from vendors, but also facilitate interoperability and cross- training, further lowering cost and improving supportability. For example, it is simply impossible to actualize robust Cybersecurity 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 (TCO).* It remains in our collective best interests to continue that trend.

2. *Agencies are the caretakers of the data that they transact.* The citizens of Maine trust their government with an immense cache of their personal data. It is essential for the State to reciprocate that trust with the best possible stewardship of that data. Further, quality information is critical to effective government decision-making and fulfilling the government's obligation to its citizenry. To achieve this goal, authoritative sources of particular data elements must be defined, and documented, across all I.T. platforms, irrespective of the department/agency. Not only that, the stewardship and governance of such data elements must be defined as well. Data exchanges must be conducted in industry-standard Web Services. While OIT handles the technical details, the Agency business units are the fiduciary stewards of their data, and must leverage industry-standard processes in exercising that stewardship.

3. *Security & Privacy are foundational to everything else.* Citizens explicitly expect their government to protect their privacy, and secure their personal data. The State implements Security & Privacy best practices at all levels of government, to ensure the

confidentiality, integrity, and availability of its information assets. The State does everything in its power to protect its information assets from unauthorized or accidental use, leakage, disclosure, disruption, modification, and destruction. All parties, both OIT as well as Agency business units, exercise the utmost vigilance toward Security & Privacy throughout the entire lifecycle of all I.T. assets.

4. *Accessibility is a core mission.* The State is fully committed to making all its Information Assets accessible to everybody. Toward that end, the Office of Information Technology (OIT) tests all Information Assets for compliance with the following standards:
   4.1. Americans with Disabilities Act 1990[1]
   4.2. ADA Amendments Act 2008[2]
   4.3. Section 508[3]
   4.4. W3C WCAG 2.1[4]

5. *Centralize Authentication; Federate Authorization.* Authentication of user and device identities must be centralized in order to improve service, enable single credential and/or single sign-on, and reduce application support costs. Centralization of authentication permits appropriate management and security controls to be applied universally. To that end, Microsoft Active Directory (A.D.) remains the State's standard directory product. Any net-new technology products must consume authentication from the State of Maine enterprise A.D. This must be accomplished on-demand, via either ADFS-SAML, or through OIT's Enterprise LDAP service. Under no circumstances will the State extend or modify its A.D. schema, or entertain any trust relationship with any other directory, or grant directory administration privilege to another party. However, individual applications and appliances are free to maintain their own dedicated authorization (roles & privileges) modules.

   OIT has launched an initiative for a centralized Enterprise Constituents Portal for citizens, businesses, and nonprofits. Once the Portal is fully operational, all existing externally-facing applications are expected to consume external authentication and identity proofing from the Enterprise Portal. This means that any product proposed by the Provider must conform to modern open standards for Authentication (such as OpenID 2.0, OAuth 2.0, SAML 2.0, etc.).

6. *First reuse; then buy; then build.* Clearly, the best value to be extracted from sunk 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 must 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 leverages additional capabilities of products it already

[1] https://www.eeoc.gov/eeoc/history/35th/1990s/ada.html
[2] https://www.eeoc.gov/laws/statutes/adaaa.cfm
[3] https://www.section508.gov/
[4] https://www.w3.org/TR/WCAG21/

owns that are still supported by their vendors.

If it is conclusively determined that an existing I.T. product cannot meet current requirements, then the State explores an off-the-shelf product that comes the closest to satisfying such unmet requirements. The State modifies its workflows and business processes in order to utilize the off-the-shelf product, but reuse and buy are still preferable to creating a custom product exclusively for its requirements.

Only if there really does not exist any off-the-shelf product that comes even close to meeting its requirements does the State explore building a custom product.

7. *Choose new products carefully to support modernization.* Choosing new products without adequate due diligence results in increased cost, 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 enhances interoperability, for there are fewer moving parts to interface with. This improves support, for there exists a higher headcount per technology option. This increases economies-of-scale, for there exists higher market share per technology option, directly leading to increased pressure on vendors for deeper discounts, dedicated training, etc. Taken together, limiting the variants of technology options reduces I.T. costs, and improves service. As we seek products in line with our mission, vision, and goals, we will seek products offering modern architecture features (Modularity, Scalability (both Horizontal & Vertical), Composability, Extensibility, and Configurability). Each element will be part of the foundational building blocks for future development and the long-term architecture.

The marketplace continues to explode with new products. Clearly, no single entity, least of all the State, can afford to sample them all indiscriminately. That said, the modernization of IT products and services for the State as a whole also cannot allow itself to fall too far behind the technology curve, lest it deprives itself of viable superior options. Therefore, the State charts a modernization course that both filters out the hype, and yet leverages lasting trends in performances with the potential to deliver higher returns on resource investment The product selection criteria is as follows, in descending order of importance:

7.1. Ability to Meet Requirements
7.2. Cybersecurity, Privacy, & Accessibility
7.3. Customer Value (Return on Investment)
7.4. Installed Base within the space supporting modularity
7.5. Supportability and Stability
7.6. Modern Architecture (Modularity, Scalability (both Horizontal & Vertical), Composability, Extensibility, and Configurability)
7.7. Sustainability (Technical Viability)
7.8. General Excellence, Standards-Compliance, and Market Position
7.9. Alignment with Long-term Architecture

Ability to Meet Requirements commands the highest weight. *Cybersecurity*, *Privacy*, and *Accessibility* remain core to our mission across-the-board. *Customer Value (Return on Investment)* considerations are holistic, not just the one-time cost of acquisition, but a best estimates of the lifetime Total Cost of Ownership (TCO) over the life cycle of the product. If a product has a large installed base within the State, and the State is already comfortable supporting it, it makes sense to continue with that product, and negotiate a deeper volume discount from the supply chain/vendor. *Modularity* means that a product natively accommodates small independent components. *Scalability* refers to the capacity of a product to start small but grow in scope and extent to keep pace with increased demand. Scalability is of two types. *Horizontal Scalability* refers to addition of more units, whereas *Vertical Scalability* refers to adding more power to the individual units. *Composability* means that a product is built out of sub-components that can be selected and assembled in various combinations to satisfy specific business requirements. *Extensibility* means that a product has the native capability to be extended with additional elements and features *Configurability* means that the product allows low/no-code realization of diverse use cases, without professional customization or re-engineering. *Sustainability (Technical Viability)* refers to the capacity of a product to thrive in a rapidly changing technology ecosystem. The State favors positions of *Excellence, and Standards-Compliance* in the marketplace. Finally, the State selects products that are in *Alignment* with its *Long-Term Architecture*.

8. *Be Cloud Smart.* For both COTS and Custom products, the hosting decision must carefully consider the following three options: Public Cloud, OIT Housing, and OIT Hosting. Each option must be evaluated, and the final decision made based upon the combined score of TCO, functionality/usability, and Cybersecurity. This applies for both new assets as well as replacement of existing assets.

Here are some of the considerations in evaluating the TCO amongst Public Cloud, OIT Housing, and OIT Hosting. The Public Cloud is more likely to yield economies-of-scale, expense pegged to actual usage, as opposed to the peak provisioning, and reduced initial capital outlay. However, the Public Cloud also may create other challenges, such as regulatory compliance, network latency, and integration with the on-premises ecosystem. OIT Hosting offers the tightest possible integration with the on-premises ecosystem, and minimizes network latency. OIT can also act as an Infrastructure-as-a-Service provider within the State of Maine Azure-Gov and Amazon Web Services (AWS)-Gov tenants. Irrespective of the hosting decision, Data remains a strategic asset for the State, and the State retains sovereign ownership of its own data at all times. For Public Cloud hosting, at the end of the engagement, the vendor must return back the State data at a mutually agreed-upon format.

To the extent the Public Cloud is chosen, the order of preference is:

8.1. Software-as-a-Service
8.2. Platform-as-a-Service
8.3. Infrastructure-as-a-Service

This sequence reflects both the order of implementation difficulty, as well as the distribution of Cybersecurity liability.

Initial Issue: 11 November 2008
Latest Revision: 6 March 2024
Point-of-Contact: Enterprise.Architect@Maine.Gov