State of Michigan
Administrative Guide to State Government

POLICY 1360.00 Systems Engineering Methodology

Issued: June 4, 2009
Revised: October 13, 2021
Reviewed: October 31, 2024
Next Review Date: October 31, 2025

FUTURE EFFECTIVE DATE

The "revisions" to this policy, found in Ad Guide Policy Communication 10/22/2021, are effective six months from the "revised" date above.

APPLICATION

This policy is intended for statewide compliance and applies to all Executive Branch Departments, Agencies, Trusted Partners, and Boards or Commissions using state of Michigan (SOM) information technology (IT) resources.

PURPOSE

This policy provides direction for the development, enhancement and maintenance of new and existing IT enabled solutions for the SOM. It also outlines specific responsibilities for Agency Directors, the Director of the Department of Technology, Management and Budget (DTMB), Agency Services Director, Chief Security Officer, Chief Technology Officer, Center for Shared Solutions Director and the DTMB Enterprise Portfolio Management (EPMO) Director. The EPMO Director facilitates the SUITE process while the IT Deputy Directors ensure their staff completes the DTMB processes outlined in this policy.

CONTACT AGENCY

Department of Technology, Management and Budget (DTMB)
Center for Shared Solutions (CSS)
Enterprise Portfolio Management Office (EPMO)

Telephone: 517-335-5489

Email: suite@michigan.gov

SUMMARY

The intent of this policy is to provide direction for the development, enhancement, and maintenance of IT solutions. Information systems play an essential role in delivering a variety of services to Michigan's residents. It is the partnership between DTMB and its client agencies that results in high quality and cost effective IT – enabled solutions that meet a variety of public sector business needs.

The System Engineering Methodology (SEM) is a component of the State Unified Information Technology Environment (SUITE). The SEM provides direction for DTMB and agency managers and staff, including contracted resources. It is sufficiently flexible to cover new projects, enhancements, and maintenance activities of all sizes.

SEM consists of generic industry standard stages of the system development life cycle: initiation/planning, requirements definition, functional design, system design, construction, testing, and implementation. This methodology describes each stage of the system development lifecycle and specifies the roles and responsibilities of participants. The SEM is sufficiently flexible for use in various product development approaches, including but not limited to agile, waterfall, and hybrid approaches as well as implementation of Commercial Off the Shelf (COTS) and Software as a Service (SaaS) solutions.

For specific direction, see the public facing SUITE website.

Additional information and training opportunities can be found on the SOM internal SUITE website.

POLICY

All SOM agencies are required to follow SEM for all IT projects.

Agency Director

The Agency Director is ultimately responsible for the operation of and risks to system and business units within his or her organization. In this role as a System (or Business) Owner, the Agency Director, or his or her designate, shall ensure:

- A business case for each proposed project or program, including identification of benefits of completing the project or the risks of not completing the project.
- Alignment to agency goals.
- Appropriate funding for each proposed project or program.
- Executive sponsorship for each proposed project or program.
- Availability of sufficient and knowledgeable resources, including subject matter experts (SME), business process analysts, testers, policy experts, data stewards and trainers.
- The data is correctly categorized, per SOM 1340.00.150.02 Data Classification Standard.
- Availability of resources authorized to test, approve and accept project deliverables (reference SEM Testing Manual).
- Availability of individual(s) to act as application system owner(s).

Agency Application System Owner

- An Agency Application System Owner has direct responsibility for a system and is responsible for gathering information and providing management recommendations on the resources required to meet operational objectives. The Agency owns the application system and has the ability to assume and/or delegate the responsibility. While no one person is likely to know all the details of a system and its operations, it is the responsibility of the Agency Application System Owner to ensure there is someone with the knowledge and authority to maintain the operation and security of the application. Responsibilities, which may be the direct

responsibility of the Agency Application System Owner or delegated to another person within the organization, include:

- The ability to express the overall purpose of the system.
- Possessing sufficient details of the system to be able to manage the day-to-day business operations of the system.
- Possessing sufficient details of the system and relevant processes so as to manage the development and continued maintenance of desk procedures for business staff that operate the system on a day-to day basis.
- Exercising authority to make final decisions in situations where system information is inaccurate after appraising the customer impact as well as the resources and time available.
- Exercising authority to provide final approval for implementation for all changes to the system.
- Possessing sufficient understanding of the application system to recommend improvements to the system to maintain an efficient and accurate business process providing customer-oriented information.
- Developing and maintaining a system business continuity plan, including business operating procedures, consistent with Administrative Guide Policy 1340 Information Technology Information Security Policy, Section 070, Contingency Planning (CP), and Administrative Guide Procedure 0240.08 Continuity of Operations (COOP) Plan.
- Conducting periodic reviews of system operations to ensure they are working as intended.
- Conducting periodic reviews of the data to ensure it is accurate.
- Coordinating periodic reviews to ensure acceptable levels of documentation – including audits and controls to ensure data integrity – and procedures for operating and maintaining the system.
- Establishing and maintaining business processes.
- Developing specifications for what the system will and will not do (including reporting).
- Ensuring there is a policy and process for granting access to the system and a process for periodic review of the access (reference SOM 1340.00.020.01 Access Control Standard).
- Ensuring the administration of training development and presentation for all staff that may update or use the information in the system (reference the SEM Manual, Activity 7.7, Develop Training Plan).

- Ensure applications meet the requirements set forth in the Authorization to Operation (ATO) policy and process (SOM 1340.00.150.01 Risk Assessment Standard).

DTMB Director

As a System Development Provider, the DTMB Director shall seek to ensure:

- Agencies are provided with a governance team consisting of members from DTMB service areas:
  - To whom project and operational metrics are provided.
  - Through which decisions about the project or system – escalated issues – can be resolved.
- Agencies are provided information and recommendations about the best technical approaches to meet business needs.
- Agencies are provided reliable and cost-effective technical solutions by researching the applicability of commercial off the shelf (COTS) solutions and other shared IT solutions (reference SEM Manual, including COTS Planning Considerations (page 32) and Appendix C, Investigating Alternative Solutions).
- Agencies are provided with a projected cost for the development and maintenance of a project, including an estimate with sufficient detail to understand the breakdown of work, as well as an outline of the total cost of ownership of the IT product.
- A mechanism is in place to collect, track and mitigate and/or resolve application and hardware vulnerabilities (reference SUITE Project Management Manual, page 83).
- A process is in place to resolve system issues and communication outcomes of the process to Agency Application System Owners.
- Agencies are provided appropriate levels of technical support for ongoing operations (reference SUITE System Maintenance Guidebook, Page 4).
- Coordination and communication of all approved changes to the project/system to the Agency Application System Owner and stakeholders agreed upon by him/her and DTMB.
- Opportunities for Agency and DTMB personnel to become educated in and use the State Unified Information Technology Environment (SUITE), SEM, Control Objectives for Information Technology (COBIT) and their associated products.
- Projects are resourced correctly with:
  - Project managers commensurate with the project size, complexity and importance.
  - Team members that are skilled or adequately trained in the technologies used.
  - Appropriate tools to complete the assigned tasks.

- Application development standards that maintain data integrity and security are developed, maintained, and followed in alignment with SOM 1360.00.10 Application Development Management Standard.
- An IT disaster recovery plan, including an agency funded "recovery time objective" and the "recovery point objectives" – is required, developed and maintained in alignment with Administrative Guide Policy 1340.00 Information Technology Information Security, Section 070 Contingency Planning (CP) and SOM 1340.00.070.02 Information Technology Disaster Recovery Planning Standard.
- All IT resources, including third-party resources, are managed to afford the SOM the best value for the contractual cost.
- Ensure applications meet the requirements set forth in the Authorization to Operate (ATO) policy and process (SOM 1340.00.150.01 Risk Assessment Standard).

DTMB Enterprise Portfolio Management Office (EPMO) Director

As an Investment Management and 3PMM Project, Program, and Portfolio Management Provider, the DTMB EPMO Director shall ensure:

- Monitoring and reporting on SUITE compliance, including consistent and effective investment management and project, program and portfolio management, application of Systems Engineering Methodology (SEM) transparency of proposed IT projects/programs, and IT project spending for the SOM enterprise.

TERMS AND DEFINITIONS

Agency

The principal department of state government as created by Executive Organization Act, P.A. 380 of 1965.

Availability

Ensuring timely and reliable access to and use of information and assuring that the systems responsible for delivering, storing, and processing information are accessible when needed, by those who need them.

Data/Information

State of Michigan agency information. No distinctions between the words "data" and "information" are made for purposes of this policy.

Data Owner

An individual or organization – usually a member of senior management of an organization – who is ultimately responsible for ensuring the protection and use of data.

Data Steward

An individual who is accountable for data assets from a business perspective, including data management, data quality, and alignment with enterprise data standards.

Information Technology (IT)

Refers to software, hardware, networking, Internet of Things, and telecommunication products and services that the state uses to store, manage, access, communicate, send and receive information. IT also refers to data, voice and video technologies. The determination of whether something falls under IT is not dependent on cost (i.e., could be a free service) or whether the product or service is hosted on state systems.

Examples of IT products or services include, but are not limited to, the following:

- On-premises, commercial-off-the-shelf (COTS) software applications installed on state systems (e.g., Adobe Acrobat).
- Externally hosted, COTS software applications installed on a vendor's system (e.g., DocuSign, Salesforce, etc.).
- Custom developed software applications (e.g., DHHS' CHAMPS system).
- Software-as-a-Service (SAAS) applications hosted by a vendor (e.g., LexisNexis, Survey Monkey, etc.).
- Subscription-based information services (e.g., Gongwer, Gartner, etc.).
- Social media accounts (e.g., Twitter, Facebook, etc.).
- Mobile applications (e.g., iTunes).
- Server hardware and software used to support applications such as database, application/web servers, storage systems, and other hosting services (e.g., Dell EMC PowerEdge Blade server).
- Hardware devices (e.g., laptops, tablets, smartphones, etc.).
- Data, voice, and video networks and associated communications equipment and software (e.g., Cisco routers and switches).
- Peripherals directly connected to computer information systems (e.g., Ricoh scan printers, printers).
- Internet of Things (IOT) are objects with electronic components that include processing and networking capabilities designed to enhance the functionality of the object by leveraging communications over the internet (e.g., ADT Security, smart thermostat, software-enabled lab equipment, refrigerator with an LCD screen, etc.).
- Vendor services for software application, installation, configuration, development and maintenance, including staff augmentation arrangements (e.g., CNSI resources assisting with maintenance and support of the DHHS CHAMPS system).

To utilize or source a product or service that includes components that meet the definition of Information Technology, the agency shall engage with the designated General Manager, or Business Relationship Manager for consultation on the need for DTMB IT services, (e.g., Cyber Security, Agency Services, Enterprise Architecture, Telecom, etc.).

Integrity

Guarding against improper information modification and/or destruction, ensuring information has not been altered by unauthorized people and the assurance that the information can be relied upon to be sufficiently accurate for its purpose. Integrity considers all possible causes of modification, including software and hardware failure, environmental events, and human intervention.

Methodology

A system of principles, practices and procedures applied to a specific branch of knowledge. A documented approach for performing activities in a coherent, consistent, accountable, and repeatable manner.

Program

Group of related projects and activities with the same or similar objectives managed in a coordinated manner to obtain benefits not available from managing them individually. A program is also known as a master project with subprojects.

System Development Lifecycle

Industry standard stages include initiation/planning, requirements definition, functional design, system design, construction, testing, and implementation.

System Owner

From an enterprise perspective, the unit that funds and has approval authority for a project. From an application perspective, individual(s) that has ultimate responsibility for a system and is responsible for gathering information and providing management recommendations on the resources required to meet operational objectives.

Trusted Partner/ Business Partner

A person (i.e., vendor, contractor, third party, etc.) or entity that has contracted with the SOM to perform a certain service or provide a certain product in exchange for valuable consideration, monetary, or goods and services.

AUTHORIZATION

Authority

This policy obtains its authority from:

- The Administrative Guide to State Government.
- Administrative Guide Policy 1305 Enterprise Information Technology.
- DTMB IT Technical Policies, Standards and Procedures, which can be found on the DTMB Intranet.
- Public Act 389, Section 115, effective December 19, 2018 regarding IT services.
- Public Act 207, Section 830, effective June 21, 2018 regarding appropriations.

Enforcement

All enforcement for this policy shall be in compliance with the standards and procedures of Administrative Guide Policy 1305 Enterprise Information Technology.

Developing Standards and Procedures for this Policy

All requirements for developing standards and procedures for this policy shall be in compliance with Administrative Guide Policy 1305 Enterprise Information Technology.

Exceptions

All exception requests to this policy must be processed in compliance with Administrative Guide Policy 1305 Enterprise Information Technology.

Effective Date

This policy will be effective, unless otherwise noted, upon signature of the Administrative Guide approval memo by the DTMB Director.

***