Assessing Cloud Computing Service Models for Child Welfare Information Systems

May 2021

Table of Contents

I. Introduction

This document reviews elements that should be considered when evaluating different cloud computing service models and strategies in association with a Comprehensive Child Welfare Information System (CCWIS) or other child welfare information system implementation.

Cloud Service Providers (CSP) are companies that offer their customers a range of cloud-based solutions, including infrastructure, storage, platforms, business applications, and network communication services. This toolkit reviews different cloud computing service models supported by CSPs and examines the primary services (infrastructure-as-a-service, platform-as-a-service, and software-as-a-service) to assess their possible strengths and weaknesses for use in a child welfare information system. Each service model is examined across a range of technical and non-technical factors.

For title IV-E agencies (agencies) considering a CCWIS implementation, this toolkit may be used to inform the selection of a cloud computing service model that may be eligible for federal financial participation (FFP) and possibly meet federal regulations for CCWIS. [1] [2] The federal regulations for CCWIS establish core project and design requirements that must be implemented to meet requirements for FFP. This toolkit crosswalks CCWIS project and design requirements, specified in 45 CFR §1355.52 and 45 CFR §1355.53 respectively, with cloud computing service model considerations. To help in decision-making, agencies should consider the CCWIS requirements with the information presented in this document.

II. Service Model Overview

Definitions used within the systems development community for different Cloud computing service models are often inconsistent and overlapping. Within this document, we use the definitions provided by the National Institute of Standards and Technology (NIST) in Special Publication (SP) 800-145, *The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology*.

A. Primary Service Model Definitions

1. Infrastructure as a Service (IaaS)

NIST SP 800-145 describes the elements of an IaaS service model:

> *The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over*

[1] Federal regulations for CCWIS can be found at 45 CFR §1355.50 to 59

[2] Federal regulations for federal financial participation of Health and Human Services Information Technology projects can be found at 45 CFR §95 Subpart F

> *operating systems, storage, and deployed applications; and possibly limited control of select networking components (for example, host firewalls).*

In this definition, a core aspect of IaaS is that a CSP offers consumers the ability to provision, configure, and leverage core computing resources including processing, storage, and networks. Available IaaS resources often include virtualized servers that can be managed similar to physical computers.

2. Platform as a Service (PaaS)

NIST SP 800-145 describes the elements of a PaaS service model:

> *The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.*

Thus, for PaaS, underlying computing resources are managed by the CSP to provide an environment and set of tools in which consumers can create and host their applications.

3. Software as a Service (SaaS)

NIST SP 800-145 describes the elements of a SaaS service model:

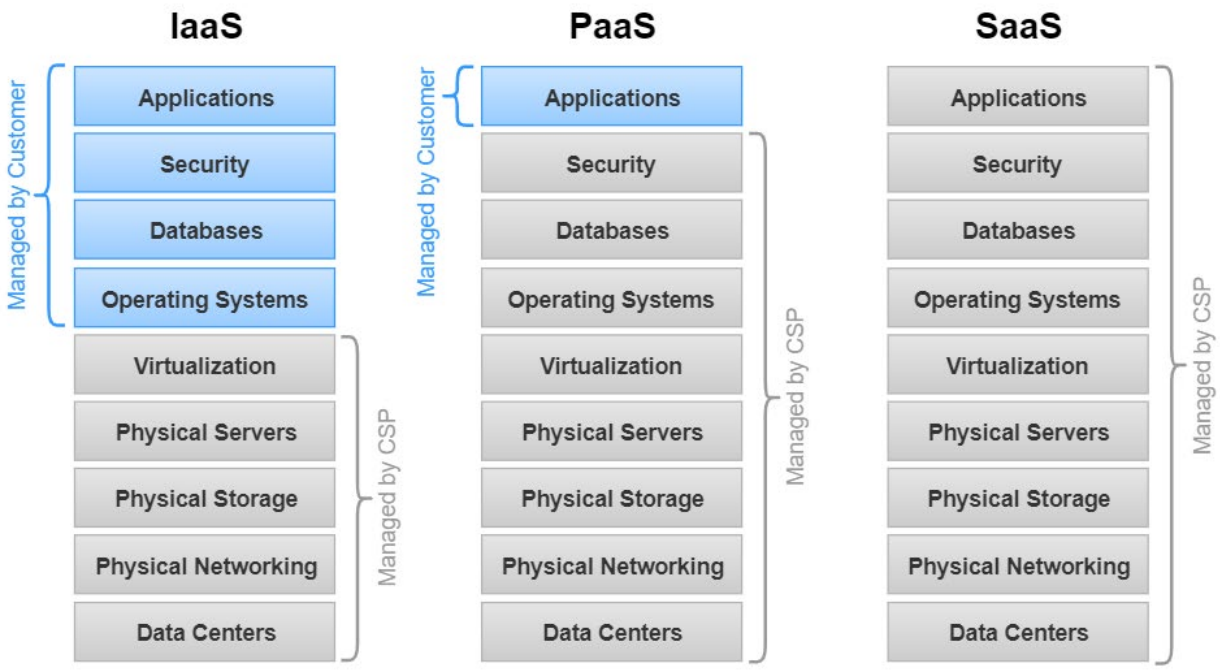
> *The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (for example, web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.*

As reflected in this definition, SaaS essentially provides consumers with the ability to use hosted application software. User configuration options provide for limited customizability.

B. Primary Service Model Comparison

Figure 1 visually represents how management responsibilities are allocated between the customer (title IV–E agencies) and the CSP for each of the primary cloud computing service models (IaaS, PaaS, and SaaS). IaaS extends the most flexibility and control to the agency, but requires correspondingly higher effort to implement, manage and operate associated systems. Conversely, SaaS provides little flexibility and control to agencies, but offers the convenience of "out-of-the-box" application functionality. PaaS is a compromise between IaaS and SaaS, providing a foundation for system implementation while managing many underlying components.

Figure 1: Service Model Management Responsibilities



C. Additional Service Models

Beyond the primary cloud computing services models, an extensive set of additional "as-a-service" models have been proposed to describe various cloud service offerings. Table 1 summarizes some of the more widely recognized additional models that may relate to a child welfare information system implementation and describes how they relate to the primary models.

Table 1: Additional Cloud Computing As-a-Service Models

Model	Description	Relationship to Primary Models
API as a Service	Provides functionality via a REST or other application programming interfaces (API)	SaaS subcategory
Backend as a Service	Provides a set of backend services for use with mobile and other web applications	Integration facility to enable access to SaaS and PaaS functionality, typically via APIs
Data as a Service (DaaS)	Provides an interface to enable access data independent of underlying platform or technology	SaaS subcategory focused on standardized data access
Database as a Service (DBaaS)	Provides database functionality to applications, with the CSP providing underlying database management.	Encompasses a variety of SaaS and PaaS RDBMS and NoSQL implementations.

Function as a Service (FaaS)	Provides an environment for developing and running server-less functions	May be considered a PaaS where the platform is a flexible application development and execution environment
Search as a Service	Provides access to search-engine functionality	SaaS subcategory
Security as a Service (SECaaS)	Encompasses a range of security-related services such as those related to identity and access management, encryption, and vulnerability scanning	May encompass a range of SaaS and PaaS
Storage as a Service	Provides a mechanism for storing data in the cloud	PaaS subcategory

As the range of cloud services continues to grow, additional "as-a-service" models are often introduced to describe and categorize these services. However, there is often no clear demarcation for these categorizations. As the number of models has proliferated, an "everything-as-a-service" (XaaS) concept within cloud computing has gained prominence. XaaS reflects the idea that an expansive set of services can be provided over the Internet.

D. Multi-Model Implementations

Cloud-based child welfare information system implementations are likely to leverage a combination of cloud computing service models. For example, custom applications are often implemented in cloud environments established through the orchestration of both underlying IaaS resource and selected PaaS offerings. Likewise, some SaaS applications have a wide range of configuration options and may incorporate application programming interfaces (APIs) that make them more flexible and extensible through adding CSP, third-party, or custom modules. Consistent with the growth of the additional "as-a-service" models, these extensible applications blur the distinction between SaaS and PaaS.

Commercial-Off-the-Shelf Software

Commercial-off-the-shelf (COTS) software can encompass any commercial software sold in the commercial marketplace that is offered to the government in the same form. SaaS can be considered a variant of COTS software that provides the commercial software over the Internet.

Likewise, just as COTS software can be implemented in a private or on-premises data center, using COTS software is an option within cloud environments. Where the COTS software is managed by the CSP itself, it should be considered a SaaS implementation.

For agencies implementing a CCWIS, a waiver of Advance Planning Document (APD) requirements may be requested to accommodate a development approach based on a COTS product.[3]

[3] Information about the waiver process can be found at https://www.acf.hhs.gov/cb/resource/acf-oa-pi1301

III. Decision Process

The selection of a child welfare information system cloud computing service model should be made within the context of the programmatic needs of the agency. The project will be executed under an information technology governance framework that will typically establish the decision-making process, define accountability, and identify responsibility for the implementation.

A. Governance Framework

Governance structures and policy will vary, but often have common elements regarding decision maker authorities, hierarchy, stakeholders and communication flows. Governance bodies may be organized into overarching categories such as:

- *Vision*. Ensure that the technology vision includes input from best practices.
- *Planning*. Facilitate key planning activities, including both strategic and tactical planning, and coordinate important strategy decisions.
- *Operations*. Create policy and standards to improve the efficiency and effectiveness of IT across the organization.

Individual governance bodies may focus on activities such as enterprise architecture, risk management and system security, standards, and project and portfolio management. Regardless of their scope, an important element of all IT governance bodies is that they incorporate input and feedback from their business stakeholders (program staff, system developers, service providers, etc.) and service recipients.

At a more granular level, a project examining different cloud computing service models will also follow a standard lifecycle. Components of the lifecycle may include:

- *Governance gates*. Represent the stage of the effort, such as concept, initiation, planning, and implementation.
- *Timeline*. Expected duration of each stage.
- *Project Artifacts*. Standardized deliverables for each stage.
- *Budget and Finance Artifacts.* Budget execution and legislative budget submittals and approvals.

More specific information pertaining to data governance is available in *CCWIS Technical Bulletin #6: CCWIS Data Quality Plan*.

B. CCWIS design requirements exemption

The CCWIS project and design requirements are specified in 45 CFR §1355.52 and 45 CFR §1355.53, respectively. And the design requirements at 45 CFR §1355.53(b) include a waiver provision that allows for modern alternative designs not specified in the regulation while exempting CCWIS functions completed before August 1, 2018. An alternative design may be approved on a case-by-case basis. This approval is pertinent since CCWIS application designs that leverage IaaS, PaaS, and (in particular) SaaS components may not always address all of the design requirements for automated functions in

45 CFR §1355.53(a). Some SaaS-based services not meeting 45 CFR §1355.53(a) requirements could potentially be leveraged based on this exemption, given an effective business case. Additionally, note that COTS products are automatically exempted from CCWIS design requirements review.[4]

C. Roles

In navigating the governance framework, and the scope and requirements of a child welfare information system implementation initiative, project planners should gather input from many parties, including stakeholder and client representatives, relevant steering committees and advisory boards, policy and technical experts, and executive sponsors.

Identifying and selecting a cloud computing service model should be performed as one component of the larger system implementation project. Ultimately, a well-instituted governance process will ensure that input is incorporated from key authorities and that systems are implemented consistent with the agency's strategic plans, enterprise architecture, compliance environment, etc.

A wide set of agency personnel will be required during planning stages of a child welfare information system, including during selection of a cloud computing service model and for determination of other architecture and design aspects of the implementation. Many of the important roles will be consistent regardless of decisions pertaining to cloud computing, but agencies should ensure that sufficient knowledge and experience in cloud computing is available during planning stages. *Cloud architects* bring specific expertise in developing and implementing cloud strategy and in architecting and designing cloud-based systems.

Agencies will need to determine the most effective means of orchestrating and managing the project and the associated roles and personnel. Agencies may consider procuring a systems integrator with responsibility for the entire child welfare information system implementation, may hire an integrator to work with multiple vendors, or may use another model.

D. Prioritization

When assessing potential cloud-based solutions, title IV–E agencies are encouraged to develop qualitative and/or quantitative instruments that allow them to integrate multiple evaluation criteria and document their decision-evaluation process. For each criterion, the agency may establish a scale for scoring alternatives, and criteria can be weighted overall based on a prioritization process that examines the relative importance of each criterion to the success of the project. An agency that publishes and shares a clear evaluation criterion within the acquisition process, will also assist vendors with responding appropriately and reduce the risk of vendor protests during the procurement process.

The next section examines a range of considerations that agencies can use to inform criteria for evaluating cloud computing service models.

[4] See Child Welfare Policy Manual Section 6.12A Question #1.

IV. Considerations

When evaluating the relative benefits of the different cloud computing service models, the agency should consider multiple dimensions. These high-level dimensions are examined below:

- *Requirements*. This dimension examines the impact of the requirements process on the selection of a cloud computing service model. Review features and functionality, user experience (UX) and design, and enterprise architecture. Also review the relative flexibility (including customizability, configurability, and modifiability) of each model, and the degree to which each model can interoperate or integrate with other systems. The agency's examination of options should include assessment and performance considerations of the proposed service model.
- *Resourcing*. The selection of a cloud computing service model cannot be made independently of an understanding of human, budgetary and other resources available. This dimension examines costs (including affordability and total cost of ownership) for implementation, operations and maintenance (O&M), and configuration. It also examines the impact of schedule and agency staff capacity, procurement and contracting constraints.
- *Quality and Compliance*. This dimension looks at considerations for quality control, compliance with security/privacy and accessibility regulations, governance, training, data management, portability, and transition/disposition. Agencies should examine how each cloud computing service model affects the agency's ability to meet CCWIS data quality requirements found at 45 CFR §1355.52 (d).

For each element of the dimension, we provide a summary that highlights the relationship of each cloud computing service model with that element. This is followed by a discussion that elaborates the impacts. Assumptions are also specified where pertinent.

A. Requirements

1. Fit

i. Features and functionality

Model	*Summary: Features and functionality*
IaaS	Agency responsibility.
PaaS	Agency may implement custom features and functionality combined with those provided by underlying platform.
SaaS	All features and functionality provided.

Discussion:

For an IaaS solution, all features and functionality must be implemented on top of infrastructure components. For PaaS, the availability of underlying platform functionality may reduce the effort required of the agency to implement applications that meet identified needs, should that platform functionality support rather than hinder implementation of required functionality. Finally, the

established feature sets of a SaaS offerings enable agencies to assess up front how much those offerings align with functional requirements, and any compromises that may be required.

Assumptions:

For SaaS, a fixed set of features is assumed. Sometimes (for example, a negotiated custom implementation provided by a CSP), the SaaS offering may be tailored specifically to the agency.

ii. User experience and design

Model	*Summary: User experience and design*
IaaS	Agency responsibility.
PaaS	Agency responsibility.
SaaS	Provided by application.

Discussion:

For an IaaS solution, UX can be incorporated into system design and implementation (such as through a user-centered design process), leading to effectively tailored and usable systems. Conversely, effective design requires agency investment and expertise that may not be readily available, leading to poor UX. Similar to IaaS, PaaS offers the ability to implement systems with tailored designs to maximize UX. By leveraging particular PaaS components, however, the architect may constrain the range of workable designs. Finally, SaaS provides agencies with the ability to assess UX and design before committing to the product. The UX of a mature SaaS offering is typically a strength overall, but that UX may not be well tailored to specific user needs if requirements do not align well.

Assumptions:

For SaaS, an inability to extensively tailor the design and interface of the application is assumed. Sometimes (such as for a negotiated custom implementation provided by a CSP), the design and interface of the SaaS offering may be tailored specifically to the agency.

iii. Enterprise Architecture

Model	*Summary: Enterprise Architecture*
IaaS	Review for consistency with organizational standards for infrastructure.
PaaS	Review for consistency with organizational standards for platforms.
SaaS	Review for consistency with organizational standards for applications.

Discussion:

Many agencies have established Enterprise Architectures (EA) that incorporate strategic decisions and standards regarding CSP selections. For IaaS, these standards may extend to the provisioning of CSP infrastructure resources, while for PaaS, standards may encompass the use and configuration of CSP platforms. Likewise, for SaaS, the EA standards may pertain to the use and configuration of CSP applications. Architects should always align selection of cloud services with EA decisions and standards.

2. Flexibility and Customizability

Model	*Summary: Flexibility and Customizability*
IaaS	Agency responsibility. Maximum flexibility, with corresponding effort.
PaaS	Agency responsibility. High flexibility, with some trade-offs for ease of implementation.
SaaS	Minimally flexible.

Discussion:

The requirements for CCWIS automated function design specified in 45 CFR §1355.53(a) require that CCWIS automated functions are implemented under modular design principles, documented in plain language, adhere to established standards, and designed for sharing, leveraging and reuse. These design requirements directly contribute to flexibility, customizability (including modifiability), and considerations including interoperability/integration, performance, quality control, and portability.

For a system implemented on IaaS or PaaS offerings, the agency may establish a customized system. SaaS offerings provide agencies with very limited ability to customize or modify functionality.

3. Configurability

Model	*Summary: Configurability*
IaaS	Agency responsibility. Typically provides limited end user configuration options.
PaaS	Some platform configuration options, but typically few end user configurations.
SaaS	User-level configurations.

Discussion:

Software configurability contributes to the system usability and flexibility., Configurability also reduces unnecessary development and maintenance efforts, consistent with CCWIS project requirement 45 CFR §1355.52(a)(3).

Configurability by end users of an IaaS-based system is typically limited since development effort is more focused on the overall feature set. Likewise, for PaaS-based systems, user-level configurations will typically be implemented at the application level, although platforms may allow for some standard configuration options to be available to end users. Finally, available SaaS configurations are generally geared to the needs of end users.

4. Interoperability and Integration

Model	*Summary: Interoperability and Integration*
IaaS	Agency responsibility.
PaaS	Platform plus agency responsibility.
SaaS	Limited to application features and functionality.

Discussion:

The CCWIS bi-directional data exchanges and data exchange standards required in 45 CFR §1355.52(e) and 45 CFR §1355.52(f), respectively, indicate that a CCWIS must support bi-directional data exchanges with multiple systems, and for specified exchanges, leverage a single data exchange standard that describes data, definitions, formats, and other specifications. Likewise, 45 CFR §1355.52(g) requires that agencies use the same automated function or the same group of automated functions for all title IV-E eligibility determinations. Thus, agencies implementing a CCWIS should prioritize interoperability and integration when considering CSP alternatives to support the data exchanges and to avoid duplication of automated functions.

The CCWIS automated function design requirements in 45 CFR §1355.53(a) require that CCWIS automated functions are designed for sharing, leveraging and reuse. These elements also support interoperability and integration.

For an IaaS implementation, interoperability and integration elements are fully the responsibility of the agency, whereas for systems implemented on PaaS offerings, some interoperability and integration elements may be provided by the platform and others are handled at the application level. Interoperability and integration options for SaaS applications are typically limited to those provided by the SaaS offering itself.

Assumptions:

For SaaS, we assume an out-of-the-box offering. Sometimes (for example, a negotiated custom implementation provided by a CSP), the SaaS offering may be configured by the CSP to interoperate with agency systems.

5. Legacy System Migration

Model	*Summary: Legacy System Migration*
IaaS	Agency responsibility.
PaaS	Agency responsibility.
SaaS	Limited to application features and functionality.

Discussion:

Migration from a legacy system to an IaaS implementation is fully the responsibility of the agency. For systems implemented on PaaS offerings, some functionality provided by the platform may facilitate migration (for example data integration and conversion features). The ability to customize IaaS and PaaS systems may allow for a gradual transfer of functionality to the new implementation. Legacy system migration options for SaaS applications are typically limited to those provided by the SaaS offering itself.

Assumptions:

For SaaS, we assume an out-of-the-box offering. Sometimes (for example a negotiated custom implementation provided by a CSP), the SaaS offering may be customized by the CSP to facilitate a legacy system migration.

6. Performance

Model	*Summary: Performance*
IaaS	Corresponds to provisioned resources plus custom implementation.
PaaS	Based on platform and provisioned resources.
SaaS	Based on software application and provisioned resources.

Discussion:

CCWIS design requirements for automated functions, as described in 45 CFR §1355.53(a), require standards and modular design principles. These design requirements directly and indirectly contribute to improved child welfare information system performance.

For an IaaS implementation, the agency typically has complete control over system performance, based on their purchase of underlying infrastructure resources combined with the architecture of their developed system. For a PaaS implementation, the agency likewise maintains significant control over system performance via the specification of platform characteristics and the design of the system. For SaaS solutions, the agency may have limited direct control over the performance of the application, but can often purchase underlying resources. Performance service-level agreements are often available for SaaS offerings.

B. Resourcing

7. Cost

i. Implementation

Model	*Summary: Implementation*
IaaS	High implementation effort and costs.
PaaS	Moderate to high implementation effort and costs.
SaaS	Low implementation effort.

Discussion:

The CCWIS efficient, economical, and effective requirement, in 45 CFR §1355.52(a)(3) and 45 CFR §1355.52(a)(4), explains that duplicative application development or maintenance efforts should not be required, and that costs should be reasonable, appropriate and beneficial.

Cost, including affordability and total cost of ownership, is a major consideration for IaaS implementations that require provisioning and configuration of all required infrastructure resources, plus custom implementation of all system functionality. The same is true for PaaS implementations to a lesser extent, as provisioning and configuration of all required platform resources is required besides custom system functionality. Implementation costs for SaaS solutions are often lower, with most costs typically associated with initial application evaluation, licensing of SaaS functionality, and configuration effort.

Assumptions:

For SaaS, we assume an out-of-the-box offering. If a negotiated custom implementation is provided by a CSP to an agency, implementation costs will be higher.

ii. Operations and Maintenance

Model	*Summary: Operations and Maintenance*
IaaS	High O&M system costs.
PaaS	Moderate to high application O&M costs, but no need to maintain the underlying platform.
SaaS	Low O&M costs.

Discussion:

IaaS-based implementations require regular, ongoing investment to continually maintain and operate the system. This includes continuous monitoring and regular patching of all underlying infrastructural components. For PaaS implementations, similar investment is required to maintain and operate the system above the platform, but platform components themselves are managed by the CSP. SaaS implementation require essentially zero agency O&M, with the application and all underlying components maintained and operated by the CSP in association with regular licensing fees.

iii. Configuration

Model	*Summary: Configuration*
IaaS	Extensive environment and system configuration required, but limited end-user specified configuration options.
PaaS	Extensive platform and/or system configuration required, but limited end-user specified configuration options.
SaaS	End-user specified configurations.

Discussion:

IaaS custom system development requires significant and ongoing agency investment in configuration management (CM) activities, although developed applications, tailored for particular needs, typically require less end-user configuration. PaaS-based custom system development likewise requires costly CM effort, although underlying PaaS offerings typically offer simplified but efficient configuration interfaces. For SaaS implementations, configuration of the underlying components is managed by the CSP, and the agency is only responsible for any necessary configuration of the application itself.

8. Schedule

Model	*Summary: Schedule*
IaaS	Lengthy implementation period.
PaaS	Lengthy implementation period.
SaaS	Short implementation period.

Discussion:

Use of CSP IaaS offerings provides benefits in terms of acquiring and provisioning infrastructure resources but does little to shorten the implementation effort associated with custom systems. Likewise, using standard PaaS offerings may somewhat shorten implementation time, but custom systems leveraging these offerings still have long system-development lifecycles. Implementation periods for SaaS solutions can be short once a SaaS offering has been selected; a relatively lengthy software-evaluation period is the driver behind implementation times for SaaS offerings.

Assumptions:

For SaaS, we assume an out-of-the-box offering. If a negotiated custom implementation is provided by a CSP to an agency, the implementation period will be extended.

9. Staffing

Model	*Summary: Staffing*
IaaS	Extensive system development and O&M staff required.
PaaS	Extensive system development and O&M staff required.
SaaS	No system development and O&M staff required.

Discussion:

Implementing a custom system leveraging IaaS resources requires a large set of specialized information technology staff for each phase of the system development lifecycle from inception through production launch and ongoing operations. Staffing requirements for PaaS implementations are similar but personnel required to manage components for which platforms are available can be reduced or eliminated. SaaS implementations have greatly reduced staffing requirements, as few specialized technology personnel are required after initial evaluation efforts are completed.

10. Procurement and Contracting

Model	*Summary: Procurement and Contracting*
IaaS	Review for consistency with organizational procurement policy.
PaaS	Review for consistency with organizational procurement policy.
SaaS	Review for consistency with organizational procurement policy.

Discussion:

CCWIS project requirement 45 CFR §1355.52(a)(4) requires that CCWIS costs are "reasonable, appropriate and beneficial." Government agencies, organizations and other entities must adhere to a range of policies and procedures when obtaining materials, supplies, equipment and contractual services. This extends to cloud services, including IaaS, PaaS, or SaaS solutions.

C. Quality and Compliance

1. Quality Control

Model	*Summary: Quality Control*
IaaS	Agency responsibility for quality control of all provisioned system resources.
PaaS	Agency responsibility for quality control of all application components plus configuration of platform and system interfaces.
SaaS	Agency responsibility for quality control related to application configuration and data.

Discussion:

CCWIS requirements for data, reporting, and data-quality in 45 CFR §1355.52(b), 45 CFR §1355.52(c) and 45 CFR §1355.52(d), respectively, specify that the implemented CCWIS solution must maintain and report on title IV-B and IV-E program data; data for state or tribal child welfare laws, regulations, policies, practices, etc.; and other information. This means data must adhere to rigorous data quality standards, including automated data quality monitoring and reporting. Likewise, the design requirements for automated functions in 45 CFR §1355.53(a), including modular design and adherence to established standards, also relate to quality improvement. Thus, these CCWIS requirements reinforce the importance and prioritization of data quality management when examining cloud service strategy alternatives.

IaaS custom system development requires significant and ongoing agency investment to ensure quality control (QC) across all environment tiers and for all system layers, components, interfaces and data. This also entails establishment of quality assurance processes and comprehensive test automation.

PaaS-based custom system development likewise requires a costly QC effort. Although the quality of underlying PaaS offerings is the responsibility of the CSP, planning and implementing an automated regression suite in a PaaS environment may be required. For SaaS implementations, the agency is only responsible for quality control of application data.

2. Compliance

i. Security and Privacy

Model	*Summary: Security and Privacy*
IaaS	Agency responsibility for managing the security and privacy of the implemented system, with potential inheritance of implemented infrastructure-level security controls.
PaaS	Agency responsibility for managing the security and privacy of the implemented system, with potential inheritance of implemented infrastructure and platform-level security controls.
SaaS	Agency responsibility for managing the security and privacy of application data within the implemented system, with potential inheritance of underlying application security controls.

Discussion:

The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. Depending on individual state and tribe policies, using FedRAMP-authorized services may be a requirement.

For FedRAMP-authorized IaaS, PaaS and SaaS offerings, cloud services meet baseline standards for security and privacy.[5] By leveraging these cloud services, the agency can inherit controls implemented by the CSP. For IaaS offerings, this set of controls is limited to the security of the underlying infrastructure components, but not the integration, use, or configuration of those components or the system implemented infrastructure. Similarly, for PaaS offerings, the agency is responsible for implementing security and privacy controls above the infrastructure and platform. For a FedRAMP-authorized SaaS offering, the agency is only responsible for implementing controls pertaining to using the application and the associated data, but not for the application itself or underlying components.

For agencies implementing a CCWIS, the APD review incorporates specific security requirements within the scope of Automated Data Processing (ADP) section 45 CFR §95.621(f) *ADP System Security Requirements and Review Process*. The ADP system security requires that state agencies must determine security requirements "based on recognized industry standards or standards governing security of Federal ADP systems and information processing." When agencies interface and exchange information with federal systems, they must adhere to these federal security requirements. Establishment of associated interconnection security agreements may require addressing additional security controls.

ii. Accessibility

Model	*Summary: Accessibility*
IaaS	Agency responsibility.
PaaS	Agency responsibility, sometimes constrained by CSP platform.
SaaS	CSP responsibility.

Discussion:

Agencies may have requirements to ensure that their child welfare information systems are accessible to people with disabilities.[6] Agencies implementing a CCWIS may choose to adopt federal standards, such as Section 508 of the Rehabilitation Act of 1973, as amended, which requires federal agencies to develop, procure, maintain and use information and communications technology accessible to people with disabilities.[7] For IaaS- and PaaS-based systems, adherence to accessibility requirements is the responsibility of the agency implementation team. For SaaS offerings, the underlying service must be accessible.

[5] https://www.fedramp.gov/assets/resources/documents/FedRAMP_Policy_Memo.pdf
[6] https://www.section508.gov/manage/laws-and-policies/state
[7] 29 U.S.C. 794

3. Governance

Model	*Summary: Governance*
IaaS	Agency responsibility.
PaaS	Agency responsibility.
SaaS	Agency responsibility.

Discussion:

When implementing a cloud-based information system, agencies should assess how potential support for a particular offering is constrained by existing policies, business processes and controls. Agencies should consider the overall value of each offering, the alignment of solutions with strategic plans and business objectives, and the ability to manage resources and risks in association with each solution.

4. Training

Model	*Summary: Training*
IaaS	Agency responsibility, including role-based security training.
PaaS	Agency responsibility, including role-based security training; possibly facilitated by CSP platform information.
SaaS	Agency responsibility, typically limited to user training; often leveraging SaaS training resources.

Discussion:

Information system training is a critical and often overlooked component of system implementations. For IaaS and PaaS custom implementations, the agency is responsible for developing trainings tailored to the information system. Consistent with NIST security controls, those trainings must include role-based security training for any personnel assigned security roles and responsibilities. For FedRAMP compliant SaaS offerings, the agency is responsible only for ensuring that application users are provided sufficient end-user training, and the CSPs typically provide out-of-the-box web-based training and video training that addresses these requirements.

5. Data Management

Model	*Summary: Data Management*
IaaS	Agency responsibility.
PaaS	Agency responsibility, typically facilitated by CSP functionality.
SaaS	CSP responsibility.

Discussion:

The CCWIS efficient, economical, and effective condition under 45 CFR §1355.52(a)(1), requires that the implemented CCWIS solution will need to maintain all program data required by federal, state or tribal law or policy. Thus, this data management consideration is of critical importance; the child welfare information system will need to incorporate a comprehensive data management solution.

Data management plans should encompass elements including the data categories produced and stored within the system; standards used to maintain those data; and the policies for accessing, sharing and archiving/preserving data. For IaaS-based systems, the agency must ensure that all data management requirements are implemented. This is also the case for PaaS offerings, although some platforms may provide functionality that facilitates data management (automated database backups, retention of transaction logs, etc.). For SaaS implementations, the primary responsibility of the agency is to ensure that SaaS offering comply with agency or organizational data management standards.

Assumptions:

For SaaS, we assume an out-of-the-box offering. If a negotiated custom implementation is provided by a CSP, the agency may specify changes or extensions to the base application that specifically support organization data management standards.

6. Portability

Model	*Summary: Portability*
IaaS	Portability to new CSPs or on-premises dependent on design.
PaaS	Portability to new CSPs or on-premises dependent on availability of equivalent platforms.
SaaS	Portability to new CSPs or on-premises often impossible.

Discussion:

The CCWIS design requirements described in 45 CFR §1355.53(a) dictate that CCWIS automated functions should be documented in plain language, adhere to established standards, and be designed for sharing, leveraging and reuse. Each aspect pertains to system portability.

Different CSPs often provide similar infrastructure resources. This can facilitate the efforts of agencies to port their systems implemented on IaaS offerings. Likewise, multiple CSP often provide services for the same underlying platform, thus offering the possibility of transitioning PaaS-based systems between CSPs. For SaaS unless compatibility with other products or services is specifically incorporated into a SaaS offering's feature set, CSP lock-in with continual licensing of the software must be assumed.

7. Transition and Disposition

Model	*Summary: Transition and Disposition*
IaaS	Systems generally easily transitioned between agencies and/or vendors (during contractor changeover, for example). Transition and disposition plans cover records management, data, software, and documentation, and provisioned CSP resources.
PaaS	Systems generally easily transitioned between agencies and/or vendors. Transition and disposition plans cover records management, data, software, and documentation, and provisioned CSP resources.

SaaS	Systems generally easily transitioned between agencies and/or vendors. Disposition planning must ensure that SaaS offering can meet requirements pertaining to records management and data retention.

Discussion:

IaaS, PaaS, and SaaS implementations typically provide mechanisms for transitioning systems between agencies and/or vendors, often through account management features. Disposition marks the end of an information system's life cycle, at which the system is formally retired. Disposition activities ensure that the system is terminated in a controlled manner and that key information about the system is preserved under records management regulations and policy.

The CCWIS software provision requirement outlined in 45 CFR §1355.52(h) requires that title IV-E agencies provide the federal government with copies of agency-owned software supported by federal financial participation (FFP), so agencies should ensure that their transition and disposition planning activities account for this requirement.

For IaaS and PaaS-based systems, the agency's disposition plans should specify details for archiving, deleting, or migrating/transferring all components of the system, consistent with organizational/agency requirements, laws and regulations. In considering SaaS implementations, agencies must ensure that SaaS offerings can meet disposition requirements, especially regarding data archiving and records management.

V. References

NIST SP 800-145, *The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology* (https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf)

Children's Bureau, *Comprehensive Child Welfare Information System, Technical Bulletin #6: CCWIS Data Quality Plan* (https://www.acf.hhs.gov/sites/default/files/cb/ccwis_tb6.pdf)

VI. Glossary

ADP	Automated Data Processing
APD	Advance Planning Document
API	Application programming interface
ACF	Administration for Children and Families
CCWIS	Comprehensive Child Welfare Information System
CM	Configuration management
COTS	Commercial-off-the-shelf
CSP	Cloud service provider
DaaS	Data as a Service
DBaaS	Database as a Service
EA	Enterprise Architecture

FedRAMP	Federal Risk and Authorization Management Program
FaaS	Function as a Service
IaaS	Infrastructure as a Service
NIST	National Institute of Standards and Technology
O&M	Operations and maintenance
PaaS	Platform as a Service
QC	Quality Control
RDMS	Relational Database Management System
REST	Representational State Transfer
SaaS	Software as a Service
SECaaS	Security as a Service
UX	User experience
XaaS	Everything as a Service