

**Commonwealth Office of Technology
Standard Process**

Standard Process Number: COT-078

Effective Date: 01/20/2017

Subject: COT Cloud Stage Gate Process

Standard Process Statement: The Commonwealth CIO has the responsibility to ensure the security of the Commonwealth's data and technology eco-system as well as a responsibility to optimize the investments that the Commonwealth makes in technology. Nowhere are these responsibilities more critical and the oversight more complex than in the area of cloud solutions. This standard procedure governs the formal approval process for the utilization of cloud solutions within the Executive Branch of state government.

All COT employees and contract staff shall maintain awareness of and comply with the protocols and workflow prescribed in this standard procedure.

Purpose: This Cloud Stage Gate process has been developed, in concert with state agencies, to review new projects that consider the use of cloud technology. It incorporates lessons learned (and will be continuously updated) to ensure that cloud deployment is integrated within the Commonwealth's enterprise architecture. It is designed to be used as a complement to other processes (Capital budget requests, etc.) by providing guidance, through a set of decision points. The process is designed to:

- facilitate gathering the information required to make deliberate decisions about where technology should reside and how it should be safeguarded.
- reduce the time required to move from concept to implementation, and
- provide transparent and objective criteria for decision makers.

This stage gate process divides the effort into distinct stages separated by decision points, each one being a prerequisite for the next.

Scope: For the purpose of this document only, vendor-hosted, off premise, X-as-a-Service (XaaS) and subscription (customized) applications will be collectively referred to as "cloud."

Any cloud solution that has been previously captured in the Kentucky Information Technology Standards (KITS) or has received an exception from KITS is not required to conform to this process. Any existing on premise solution proposing to move to cloud will be required to conform to this process even if the legacy system has previously received an exception or exists in KITS. A business application will be reviewed by this process if any part of the business application or business application data is proposed to reside in the cloud.

Cloud solutions offer tremendous opportunities in flexibility and agility with a potential to improve deployment economies. COT expects an ever-increasing cloud presence for the Commonwealth. However, the quality of currently available cloud solutions widely varies. Many cloud vendors have robust and continuously evolving practices they apply in the delivery of state of the art solutions. Other cloud vendors have limited cloud experience and have immature technical, security, and contract management practices associated with their new cloud offerings.

A solution that leverages a cloud product that is captured in KITS for a "new" application will require Stage Gate Review but may require additional approval. For example, Platform as a Service (PaaS) solutions may offer a broad range of application alternatives. While a common platform may support

multiple applications, application specific PaaS approval will be governed by the handling of data within each specific application. In other words, two agencies may use the same application as a platform but their use cases and the data they transmit and store may be very different.

Standard Procedure Maintenance and Compliance Responsibilities: The Office of Enterprise Technology, Division of Enterprise Architecture is responsible for maintaining and updating this standard procedure. The CIO's Office and COT leadership will enforce compliance with this standard procedure.

Review Cycle: This standard procedure will be reviewed at least every two years.

Definition(s):

Vendor Hosted:

Hosted services are “outsourced” information technology (IT) systems and functions. A hosted service provider owns and oversees infrastructure, software and administrative tasks and makes the system available to clients, usually over the Internet. [Note: a vendor hosted solution could be on premise (located at the Commonwealth Data Center) or off premise]. Some vendors are advertising “as a Service” offerings (e.g., Hardware as a Service) which do not appear to conform to the flexibility and on-demand characteristics of standard NIST definitions. For the purpose of this process, these solutions can be treated within the class of “cloud” solutions).

XaaS – “As a Service” Solutions:

- **Software as a Service (SaaS).** 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 (e.g., 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.
- **Platform as a Service (PaaS).** 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.
- **Infrastructure as a Service (IaaS).** 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 operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

Subscription Service:

The subscription business model is a business model where a customer must pay a subscription price to have access to the product/service. Any subscription service that **does not** collect user information, require identity management by the Commonwealth, or store user data is excluded from the stage gate process but must still conform to KITS / ITSC processes.

Roles and Responsibilities

Responsibility for Stage Gate process administration shall be with the Chief Architect or designee within the Commonwealth Office of Technology. Within the Stage Gate processes:

Stage Gate Process

Stage Gate Workflow and Reporting shall be the responsibility of the Chief Architect or designee.

Stage Gate 1 (Business Need)

The request for Stage Gate review, the submission of supporting documentation, and contributions to business case development/analysis will be the responsibility of the requesting agency's chief technology officer or equivalent.

The Go / No-Go decision will be the responsibility of the Director of Enterprise Architecture or designee. The Chief Architect or designee will be responsible for ensuring that data collected to support decision-making, the decision and rationale for the decision (if required), and "hand-off" to Stage Gate 2 is reported to the requestor and all COT reviewers / approvers.

Stage Gate 2 (Security)

The Go / No-Go decision will be the responsibility of the Chief Information Security Officer or designee. The Chief Information Security Officer or designee will be responsible for ensuring that data collected to support decision-making, the decision and rationale for the decision (if required), and "hand-off" to Stage Gate 3 is reported to the requestor and all COT reviewers / approvers.

Stage Gate 3 (Make or Buy)

The Go / No-Go decision will be the responsibility of the Chief Information Officer (CIO).

The Chief Architect or designee will be responsible for the administration of this process and for making recommendations regarding enterprise applications, whether a proposed solution should be considered as an enterprise application, and assisting in trade-off analysis. The Director of Enterprise Architecture or designee will also identify alternative solutions, as appropriate.

The Executive Director of the Office of Infrastructure Services or designee will be responsible for determining the business case for a "Make" decision for all infrastructure related decisions including an assessment of the impact on infrastructure shared services / costs if solutions propose moving from on premise to off premise. If on premise infrastructure alternatives are identified, the Executive Director of the Office of Infrastructure Services will prepare the business case for the "Make" option.

The Financial Data Management Branch will review the financial analysis of the proposed solution.

The Human Resources Liaison will support the personnel assessments / analysis of the proposed solution / alternatives.

The Executive Director of the Office of Application Development or designee will be responsible for developing the business case for other alternatives, if appropriate.

Cloud Procurement and Management

The Commonwealth Office of Technology shall have fiduciary responsibility for all infrastructure deployed for the Commonwealth of Kentucky's Executive Agencies whether that infrastructure is acquired as a purchase or lease or if that infrastructure is deployed by a contractor in support of a service offering.

In all cases, COT shall be responsible for specifying, managing and monitoring all platform and platform performance specifications including technical performance, geographic locations and disaster recovery plans, and service level agreements for transaction / operational performance.

In all cases, COT shall be responsible for specifying, managing, and monitoring all data hosting (whether on premise or remote) and security related issues.

IaaS: The Commonwealth Office of Technology shall be the sole acquirer and manager of Infrastructure as a service (IaaS) cloud services for Executive Branch agencies within the Commonwealth of Kentucky.

SaaS and PaaS: The Commonwealth Office of Technology shall acquire "Software as a Service" and "Platform as a Service" offerings for Executive Branch agencies within the Commonwealth of Kentucky.

It shall be the role of COT to manage data, infrastructure-like services, and security.

It shall be the role of the Agency to manage application development and testing, user acceptance testing, and application quality assurance.

A single contract manager shall act as the Commonwealth's agent with a COT technical manager and an Agency technical manager routinely reporting to that contract manager for governance.

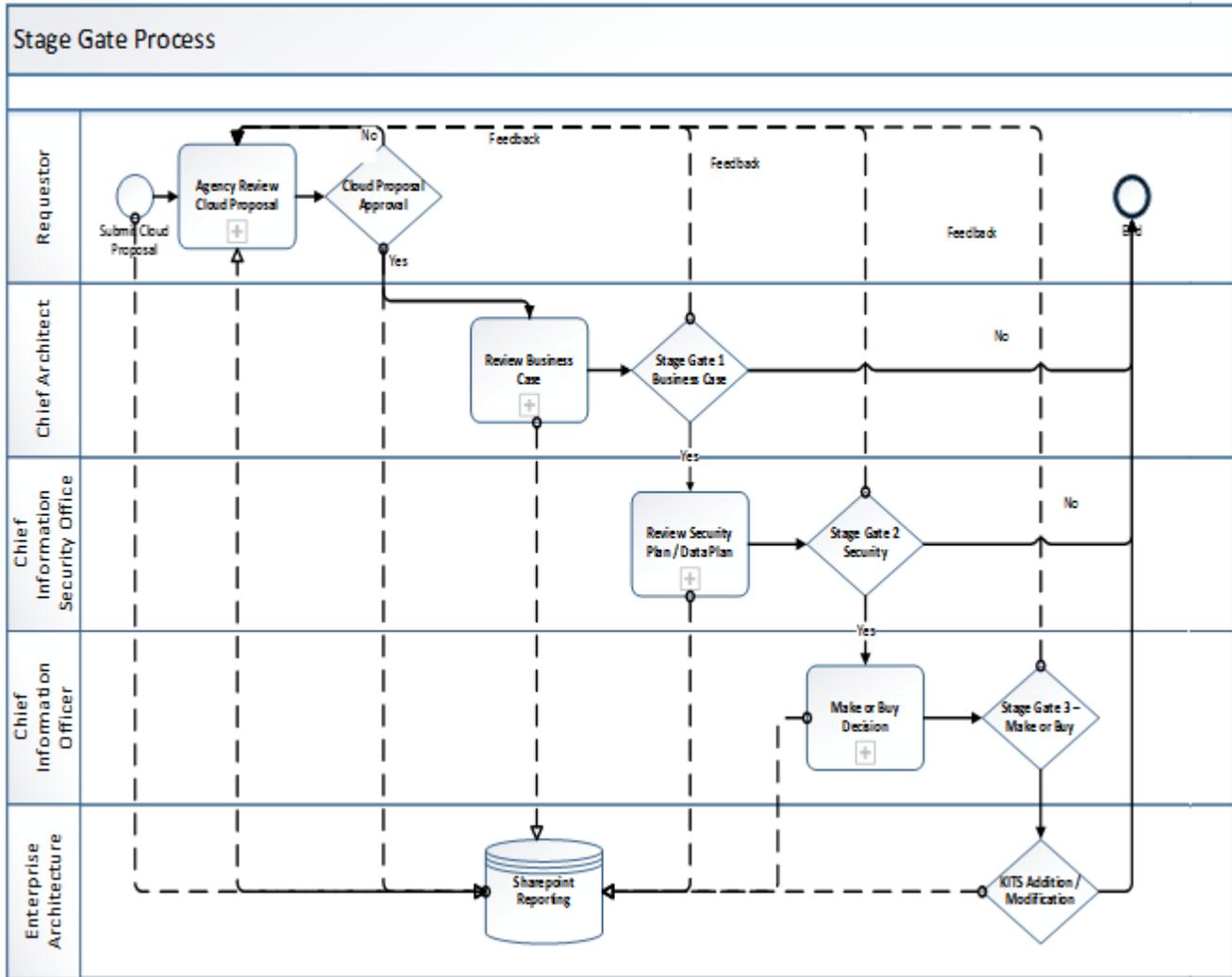
A memorandum of understanding (MOU) defining roles and responsibilities for hosted services (for the duration of the contract) shall be in place prior to contract award between COT and the agency.

Stage Gate Process

This Stage Gate is designed to be used as a complement to other processes by providing preliminary approvals in a Go/No Go format. The process is designed to facilitate gathering the information required to make deliberate decisions about where technology should reside, how it should be safeguarded, and reduce the time required to move from concept to implementation. It is also intended to facilitate inter-agency collaboration and ensure that Enterprise requirements are incorporated into project design as early as possible to eliminate waste and re-work of engineering solutions.

The stage gates are compartmentalized to review specific dimensions of project design in each stage gate. The stage gates are designed to provide feedback to acquiring agencies early in the acquisition

process. As such, it is recognized that engineering design may not be complete but the design must be sufficiently advanced to reasonably assess risk and develop planning estimates. It is expected that, pre-RFP, an agency will be able to review the basic outline of a project using the stage gate process. It is recognized that a detail engineering specification may not be developed until a contractor is chosen but it is assumed that the engineering specification will conform to the engineering estimates and constraints developed in this process.



Each stage gate must be successfully passed prior to proceeding to the next decision point. That is not to say that all questions must be closed but there must be sufficient confidence to move forward to the next decision point. It is possible to suspend or terminate the process at any point or to return it to an earlier stage.

Stage Gate 1 – Business Justification

The first stage gate is the basic need question. Requestors should provide the following information:

Business Application / Service Uniqueness. Is this request intended to replace or upgrade an existing application? If so, identify the existing application and provide a description. (The existing application description can be referenced in the business requirement description below). Is this Business Application or Service Offering currently part of the Kentucky Information Technology Standards (KITS)? Is a similar offering currently part of KITS? If this application / service offering was implemented what changes to KITS would be proposed?

Business Requirement Description. This should be a functional description of the application or business service being sought. This should include all business functions that are being sought but only those functions that are being sought. If a product sheet or website is used as a basis for the functional description, only those elements that are required for deployment should be identified. Other services may ultimately be bundled into a procurement but that will be determined by other processes / decision points.

Enterprise solution vs Agency solution. Single purpose solutions (e.g., highway construction) would not normally be considered as an enterprise solution. Identify any regulatory or funding constraints associated with the solution. (Note: the agency will provide an opinion on whether a single-purpose solution is required. Part of the analysis will be to determine if solutions can be leveraged across multiple applications).

Business User Description. This should be a description of the application or business service user demographics. Included in this description should be the type of user (citizen, Commonwealth employee, contractor, etc.), the use case of the type of user, and the number of users expected. The description of demographics should also include how users are expected to access the business service and from where. Frequency of use, number of transactions expected, “normal” business hours (if any) should be documented in this section.

User/developer/maintainer roles and responsibilities

Business process diagram (at the team or branch level – detailed software processes are not required but all stakeholders should be identified with their basic tasks outlined).

Technical Overview. This should be a technical overview of the proposed solution including a description of the required service levels from the service provider and a description of the candidate technical solution as well. IF the proposed product and service offering is known, it should be included. (Including a discussion of the physical location of provider infrastructure (if known)).

The Commonwealth’s Enterprise Architecture team may be able to help with basic research in alternatives but because of staffing limitations, it shall be the requirement of the proposing agency to identify and propose alternatives (even if those alternatives are not recommended).

Additionally, a description of data / information including any access / integration with external systems should be provided. What other systems are affected? What interfaces need to be changed? At the end of contract; What format will Commonwealth receive its data?

Financial Overview. This should provide a planning estimate for the costs of the solution including: startup costs, transition costs, and annual operating costs. Costs should include both the contracted costs and the support costs (operation or administration) to be performed by the Commonwealth. A link to the COT Total Cost of Ownership (TCO) Matrix is included [here](#). The form is not required but it does reflect the type of information that will be evaluated.

For legacy applications, the requestor should provide current cost information (actuals) including VIP billing numbers and costs (if available,) and/or contract numbers and costs (if applicable).

The requestor should discuss implementation plans, operational/security audits, and contract management processes (including SLAs) anticipated.

Discuss any special implications and consequences that would result from the approval of this request including a brief summary of the benefits that would be derived from approval cloud or vendor-hosted deployment. If consequences include any risk, address the risk mitigation plan.

The requestor must obtain approval from the senior IT officer (normally titled CTO or CIO) of their agency to begin the stage gate process,

Upon receipt of the request, the Chief Architect or designee shall:

Notify the offices of the CIO, the CISO, and the Office of Infrastructure Services that a request has been initiated.

Post the request and associated documents as they are received on a collaborative workspace for review by COT personnel and by the requestor.

Review the request and accompanying documentation for completeness. Coordinate with the requestor to provide additional information if required.

Identify any issues / alternatives to the proposed solution. (For example, if a requestor is proposing the duplication of an enterprise application or an application that may be employed by another agency, determine the necessity of the proposed solution in conjunction with the customer agency.

Review the information provided by the requestor and provide a Go / No-Go. This is not a project approval but a determination that sufficient justification and research has been conducted to move to a preliminary security overview. The decision will be published to the requestor, the CIO, the CISO, and the OIS with any conditions or questions that might accompany it,

Upon the receipt of a Go decision from the Chief Architect or designee, the Chief Information Security Officer or designee will become responsible for completing the review of all State Gate 2 issues and will coordinate directly with requestor for information. All information requested and collected shall be posted on the collaborative site.

Upon receipt of a Go decision from the Chief Architect or designee, the Executive Director or designee of the Office of Infrastructure Services shall determine if the OIS has an alternative business case (keeping the solution on premise or developing an on premise solution). Using the business case information established in Stage Gate 1, the OIS shall prepare the alternate business case (if desired) to be presented and discussed at a joint meeting with the requestor at Stage Gate 3 (Make or Buy).

Stage Gate 2 –IT / Data Security

The second stage gate in the hosted decision is a basic security question that centers on what type of data will the solution application contain/consume and where will that data reside. Requestors should provide the following information:

Data content. What data will be collected, stored, and/or transmitted by the application / solution? This should specifically identify any sensitive data (e.g., personally identifiable information (PII) or HIPAA medical information).

Data storage and movement. Is the Cloud application sending/receiving sensitive data over Internet back to COT (CDC/ADC)? How is data moved between COT and vendor DC? Between vendor DCs? Where does data reside (including what data centers or vendor locations – geographies - are anticipated to host Commonwealth of Kentucky data and will Kentucky data be comingled on a server / storage device with other customer's data? Security – SSAE16 SOC2 compliance for DC?

How is the integrity of the data protected in transit and at rest? Is data masking employed and if so, how?

Describe the security features of network connections and certificates that are being considered for use.

Note: CIO approval is required prior to the movement of any data out of state.

Backup, Disaster Recovery, and Business Continuity. The requestor will outline the backup, disaster recovery and business continuity requirements for the application / business service including the Recovery Point Objectives and the Recovery Time Objective. Is disaster recovery a built-in feature? How does it work? If it is not built-in, what is the disaster recovery process envisioned? How are data backups performed? (Via network between DCs, tape, or other

Identity Access Management. Who is responsible for IAM and how is it handled? How do users authenticate/get authorization to applications? ADFS shall be used

Access. How is the hosted application accessed? Supported browser, SFTP, SSH, etc.?

Design. Is there a thick client or middleware involved? What other systems are expected to interface / share data with the proposed application.

Upon receipt of the request, the Chief Information Security Officer or designee shall:

Post the request and associated documents as they are received on a collaborative workspace for review by COT personnel and by the requestor.

Review the request and accompanying documentation for completeness. Coordinate with the requestor to provide additional information if required.

Identify any issues / alternatives to the proposed solution.

Review the information provided by the requestor and provide a Go / No-Go. This is not a project approval but a determination that sufficient justification and research has been conducted to move to the make or buy decision. The decision will be published to the

requestor, the CIO, the Chief Architect or designee, and the Office of Infrastructure Services with any conditions or questions that might accompany it,

Upon the receipt of a Go decision from the Chief Information Security Officer or designee, the Chief Information Officer or designee will become responsible for the Stage Gate 3 decision and the Chief Architect or designee will coordinate directly with requestor, the Chief Information Security Officer or designee, for information. All information requested and collected shall be posted on the collaborative site.

Upon receipt of a Go decision from the Chief Information Security Officer or designee, the Executive Director or designee of the Office of Infrastructure Services shall refine the internal (Make) business case as required to be presented and discussed at a joint meeting with the requestor at Stage Gate 3 (Make or Buy).

Stage Gate 3 – Make or Buy/Lease

The third gate is a make-or-buy decision. This requires a high level review of the cloud solution, any resident solution, and any solution that is identified that might be installed on premise and can compete with the cloud solution.

The Chief Architect or designee shall arrange a meeting between the requestor, the CIO, the CISO or designee, and the Executive Director or designee of the OIS (if appropriate) to review the proposed solution and any alternatives if the CIO determines such a meeting is required prior to decision making. If any additional information (such as an alternative OIS proposal) is to be presented, Chief Architect or designee will ensure that it is published in the collaborative workspace per previous documents.

At the CIO direction, the Chief Architect or designee will ensure that Financial Management and Human Resources are present in the Make or Buy decision to support the cost/financial review of proposed alternatives and the strategic skill sets that may be required / available for proposed alternatives.

The CIO Make / Buy team shall consider the following questions:

Cost models COT vs Vendor

What becomes of current COT infrastructure that hosts application? Can hardware be re-purposed?

How does the Make or Buy affect our long term personnel requirements? COT shall conduct a strategic skills assessment to ensure that any technical skills that may be required for support of the hosted solution are on the personnel roadmap AND any change in required skill levels for the installed base do not negatively impact other enterprise applications / agency costs

CIO / Agency Approval

Following review of the business case and strategic assessments produced in Stage Gate 3, the results the Go / No Go decision with any comments or constraints will be forwarded to the requestor by the Director of Enterprise Architecture or designee.

In the event of a Go decision and with the understanding that a specific product / business service has been selected, the Chief Architect shall request a KITS addition / modification.

In the event of a Go decision and with the understanding that a solicitation is in process, the Chief Architect or designee shall notify the requestor that the CIO has conditionally approved the vendor hosted / cloud solution but final review and cloud addition / modification is conditional on final design. Once final design has been reviewed to ensure conformance to comments / constraints the Director of Enterprise Architecture or designee shall request a KITS addition / modification.

Assuming there is an approval, the agency and COT may proceed with the acquisition of cloud services based on the MOU and MOU roles and responsibilities.

In the event of a No Go decision, the CIO shall notify the requestor and shall indicate the reason the request was rejected.

References / Forms:

- COT Total Cost of Ownership Matrix
<https://gotsource.ky.gov/docushare/dsweb/Get/Document-349875/>
- Kentucky Information Technology Standards
<http://technology.ky.gov/Governance/Pages/KITS.aspx>
- Exceptions, Modifications and Additions to KITS
<http://technology.ky.gov/Governance/Pages/ExceptionstoArch.aspx>
- Commonwealth Office of Technology – Internet Website
<http://technology.ky.gov/Pages/default.aspx>

End