U.S. GOVERNMENT PUBLISHING OFFICE

OFFICE OF INSPECTOR GENERAL

AUDIT REPORT
REPORT NUMBER 16-21

Organizational Transformation: Composition System Replacement

September 29, 2016

U.S. GOVERNMENT PUBLISHING OFFICE
OFFICE OF INSPECTOR GENERAL

Date

September 29, 2016

To

Chief Information Officer

From

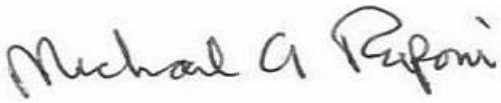
Inspector General

Subject:

Audit Report—Organizational Transformation: Composition System Replacement
Report Number 16-21

Enclosed please find the subject final report. Please refer to the "Results in Brief" for the overall audit results. Our evaluation of your response has been incorporated into the body of the report. We consider management's comments responsive to the recommendations. The recommendations are resolved and will remain open for reporting purposes pending completion of the proposed actions.

We appreciate the courtesies extended to the audit staff during the course of our review. If you have any questions or comments about this report, please do not hesitate to contact Mr. Phillip M. Faller, Assistant Inspector General for Audits and Inspections at (202) 512-2009 or me at (202) 512-0039.



MICHAEL A. RAPONI
Inspector General

Attachment

cc:
Director, GPO
Deputy Director, GPO
General Counsel
Chief of Staff
Chief Administrative Officer

Contents

Office of Inspector General

Report Number 16-21 **September 29, 2016**

Organizational Transformation: Composition System Replacement

Introduction

GPO began developing the Composition System Replacement (CSR) as a replacement for its legacy computer application—Microcomp. Microcomp uses a 30-year-old batch composition engine to compose most of the congressional documents printed and published electronically. CSR is expected to produce output in formats that provide for enhanced search, data repurposing as well as interface with Federal Digital System (FDsys). CSR will work within GPO's Enterprise Architecture (EA) as well as serve as a stand-alone application and deployed remotely at the U.S. Capitol.

OIG conducted an evaluation to determine the framework GPO followed during development of the CSR system as it pertained to EA. To accomplish our objective, we examined relevant Federal EA guidance and GPO policies and procedures. We reviewed records associated with system design, development, deployment, testing, and approval. We compared relevant guidance, policies, and procedures to activities and processes associated with the design, development, and deployment of CSR in relationship to EA. We interviewed key officials performing oversight and approval functions. We conducted the evaluation from April through September 2016 at GPO in Washington, D.C. in accordance with the Council of the Inspectors General on Integrity and Efficiency Quality Standards for Inspection and Evaluation, January 2012. Details of our objective, scope, and methodology are in Appendix A.

Results in Brief

GPO policy requires evaluation of Information Technology (IT) investments with a focus on interoperability, application portability, and scalability across networks of heterogeneous hardware, software, and telecommunications platforms, and compliance with Technical Reference Model (TRM). It also requires that the Architecture Review Board (ARB) provide guidance and assistance for development, maintenance, and management of its TRM. The review board must verify alignment with existing standards and skillset decisions, including TRM. TRM is a component-based technical framework used to categorize standards, specifications, and technologies supporting and enabling the delivery of service.

GPO is deploying CSR at the U.S. Capitol without notable incidents. Although OIG acknowledges this as an accomplishment, we believe management did not always

mitigate investment risks. Our evaluation revealed: (1) CSR was not evaluated for compliance with GPO's TRM, and (2) the ARB did not verify CSR alignment with the TRM. In addition, GPO EA policy did not reflect key changes in Federal EA guidance to include key security controls.

Recommendations

We recommend the Chief Information Office:

(1) Ensure interoperability of CSR within GPO's EA and Congress.

(2) Ensure security factors based on a risk-based framework are addressed prior to granting an Authorization to Operate.

(3) Evaluate EA policy and if appropriate revise and implement updated policy to reflect current Federal EA guidance.

Management's Response

Management concurred with the recommendations. The complete text of management's response is in Appendix C.

Evaluation of Management's Response

We consider the recommendation resolved but will remain open pending our confirmation of the final actions.

Background

Information technology (IT) plays a critical role in GPO's ability to carry out its mission. GPO began developing the Composition System Replacement (CSR) as a replacement for its legacy computer application. CSR is a composition model based on the Extensible Markup Language (XML)—a markup language defining a set of rules for encoding documents in a format that is both human readable and machine readable.

Systems development at GPO is an effort to automate activity (business processes) by using hardware, software, people, and procedures. The Chief Information Officer (CIO) is the Designated Accreditation Authority for GPO systems and responsible for reviewing and issuing management approval to operate the systems. The CIO is responsible for overall management of IT resources and for establishing specific procedures and methodologies for conducting project/system development in the GPO environment. Such responsibility includes developing and maintaining an Agency-wide IT System Development Policy. The CSR Program Manager manages overall program activities and is appointed by the Office of the Chief Technical Officer (OCTO) or by the Office of the CIO. The CSR Program Manager is a member of the OCTO staff, also known as Programs Strategy and Technology.

Management Control Guidelines

GPO requires[1] that management controls provide reasonable assurance and safeguards to protect assets against waste, loss, unauthorized use, and misappropriation. The guidance states that GPO must maintain effective systems of accounting and management control. The policy states that internal controls are the organization, policies, and procedures used to reasonably assure that resources are used consistent with Agency mission and resources are protected from waste, fraud, and mismanagement.

The Government Accountability Office (GAO) *Standards for Internal Controls in the Federal Government*, September 2014, require ongoing monitoring in the course of normal operation and the use of control activities. Control activities are the policies, procedures, techniques, and mechanisms that enforce management's directives and address related risks.

Prior Related Audits

OIG Report Number 16-11*, Independent Verification and Validation of GPO's Composition System Replacement,* dated March 30, 2016*.* Through a contract, OIG conducted an Independent Verification and Validation (IV&V) of CSR to identify development risks early in the life cycle and make recommendations for mitigating

[1] GPO Instruction 825.18A, *Internal Control Program*, dated May 28, 1997.

or lessening those risks. OIG reported that GPO had made great strides as a result of the project team's collective focus on testing and adoption of an iterative approach to delivery. The audit identified several high risks that could result in increased development costs and potentially impact product capabilities. OIG made 29 recommendations to create a road map for improved delivery and a baseline for future IV&V assessments of the development practices for the CSR project.

OIG Report Number 12-19*, Enhanced Architecture Maturity Could Better Guide GPO's Transformation,* dated September 28, 2012*.* OIG conducted an audit to determine the extent to which GPO assured that its Enterprise Architecture (EA) was used to guide and constrain ongoing development and support of GPO's strategic transformation. We reported that GPO had developed and implemented an EA policy, created the EA Program Office, appointed a Chief Architect, used an automated tool containing reference models to assist in developing EA, and from 2008 to 2010 established an Architect Review Board (ARB). In 2010, GPO performed a self-assessment using GAO's framework and determined a maturity level of Stage 4 in the GAO framework. The highest level of maturity is Stage 6. Stage 4 represents completing and using an initial EA version for targeted results. We compared GPO's progress with the GAO framework. Based on both the audit and GPO's self-assessment in 2010, management did not fully expand and evolve EA and its use for transformation and optimization.

Results and Recommendations

GPO established policy that would mitigate risk that its IT investments support mission operations and modernize the environment. However, key policy provisions were not always followed. For example, (1) GPO did not evaluate CSR for compliance with the TRM, and (2) the ARB did not verify alignment with the TRM. In addition, GPO policy did not reflect key changes in Federal EA guidance to include key security controls. The details are reflected below.

CSR Not Evaluated for Compliance with GPO's TRM

GPO could not demonstrate it evaluated CSR for compliance with its TRM or the interoperability between cross-agency architectures/implementations (U.S. Capitol). GPO Directive 705.31A, GPO Enterprise Architecture Policy, dated December 16, 2013 states that management must evaluate IT investments with a focus on interoperability, application portability, and scalability across networks of heterogeneous hardware, software, and telecommunications platforms, and compliance with the TRM. The Directive further requires that Configuration Management and Change Management processes must be integrated with the requirements established by the Technical Configuration Control Board (TCCB) and TRM.

GPO last updated its entity-wide TRM on September 13, 2013. By definition, the TRM is a component-driven, technical framework categorizing technologies to enable the delivery of service. Aligning agency capital investments to the TRM standardized technologies allows interagency discovery, collaboration, and interoperability.

GPO documentation reveals that CSR is a composition model based on Extensible Markup Language (XML) and capable of generating output in data formats to support enhanced search and repurposing of data and interface with GPO's Federal Digital System (FDsys) for content submission and dissemination.

The table below provides the OIG analysis of key TRM Service Areas, Service Categories, and Service Standards that address standardization of Exchange Package and Data Sharing.

Table 1. Analysis of Key TRM Service Areas

Service Area	Service Category	Service Standard	OIG Analysis
Data Transformation	Language Transform	Xmetal	Documented
	eXtensible Stylesheet	Xmetal	Documented
Data Exchange	XML	eXtensible HyperText Markup Language	Partially Documented
		XML Process Definition Language	Partially Documented
		XML Digital Signature Standards	Not Documented
		Standard Generalized Markup Language	Documented
Development Languages	Platform Dependent	.Net	Not Documented
		SQL	Not Documented
		Unix / Linux Scripts	Documented
		Java	Not Documented
	Platform Independent	PERL	Not Documented
		Python	Not Documented
Search Services	Search Engine	FAST search engine	Not Documented
		Lucene search engine	Not Documented

ARB Verification with the TRM

The ARB did not verify CSR alignment with the TRM. GPO policy[2] requires that the ARB ensure that acquisition of IT throughout the Agency align with its EA and strategic priorities. The ARB provides guidance and assistance in the development, maintenance, and management of GPO's TRM as well as verifies alignment with existing standards and skillset decisions, including the GPO TRM. Managers stated the ARB no longer holds meetings.

Federal EA Guidance

An OIG comparison of GPO EA policy[3] to Federal EA guidance entitled Federal Enterprise Architecture Framework (FEAF), version 2, dated January 2013 revealed key differences. The comparison is detailed below.

GPO policy follows the Consolidated Reference Model Version 2.3 that the Office of Management and Budget (OMB) released in 2007 and included a revised TRM as part of the set of interrelated "reference models" framework. The TRM leverages a common, standardized vocabulary, allowing interagency discovery, collaboration,

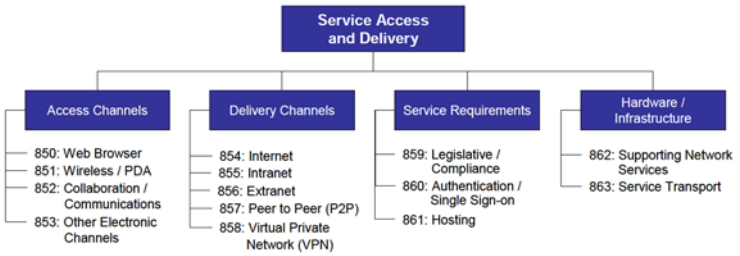
[2] GPO Directive 705.31A, *GPO Enterprise Architecture Policy*, dated December 16, 2013.

[3] GPO Directive 705.31A, *GPO Enterprise Architecture Policy*, dated December 16, 2013.

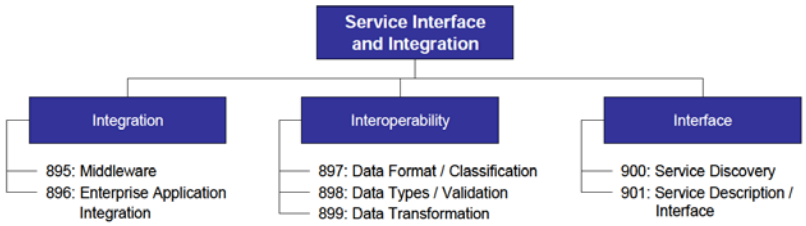
and interoperability. Organized in a hierarchy, the TRM categorizes the standards and technologies that collectively support the secure delivery, exchange, and construction of business and application Service Components that may be used and leveraged in a component-based or service-oriented architecture. Figure 1 illustrates the service areas and related service categories contained in the TRM.

Figure 1. Technical Reference Model

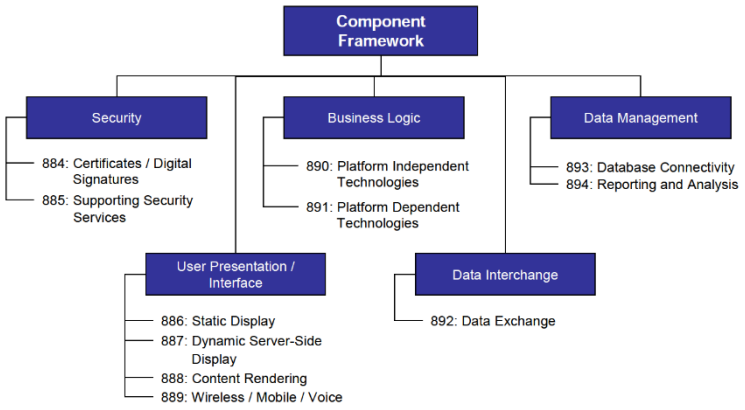
Service Area: Service Access and Delivery

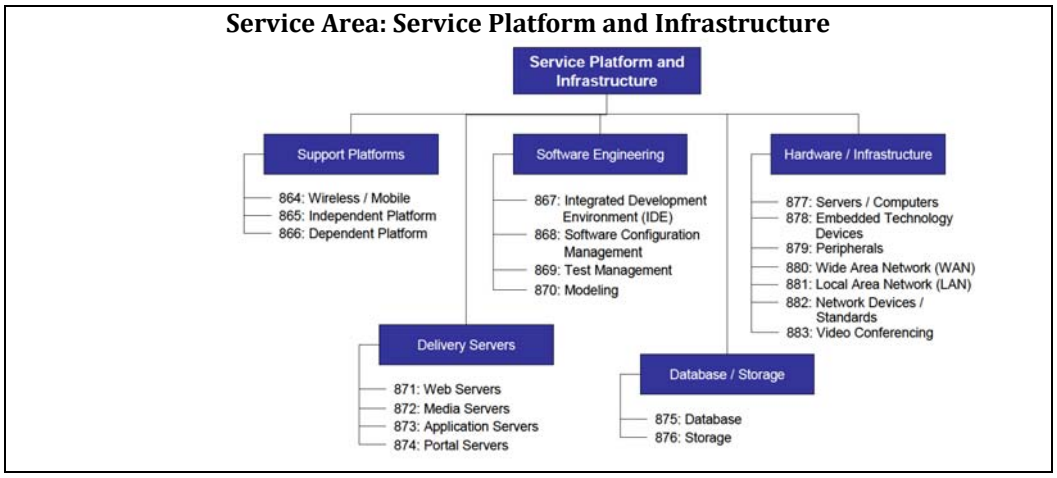


Service Area: Service Interface and Integration



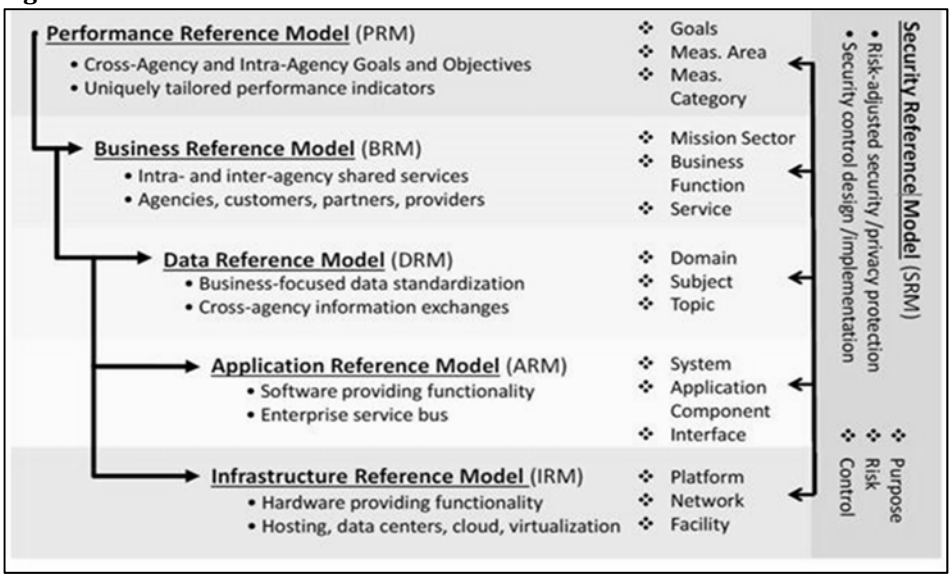
Service Area: Component Framework





The most recent Federal Enterprise Architecture guidance is the *Federal Enterprise Architecture Framework*, version 2, dated January 19, 2013. Starting with the 2013 policy, the four reference models were regrouped and expanded to six. As Figure 2 depicts, the TRM was removed from Federal EA policy.

Figure 2. Consolidated Reference Model



Security is integral to architectural domains and at all levels of an organization. As a result, the Security Reference Model was added and provides a common language and methodology for discussing security and privacy in the context of federal agencies' business and performance goals. Following are several examples of key security factors not addressed at the system or application level:

- Integrity–Assurance the data is not altered from its original content during its storage or transmission.

- Availability–Assurance the data will be ready for use when required.
- Cross-domain requirements, network connection rules, and cryptographic key management information.

GPO policy states all Configuration Management and Change Management processes must be integrated with the TCCB and TRM. IT investments must be evaluated with a focus on interoperability, application portability, and scalability across networks of heterogeneous hardware, software, and telecommunications platforms, and compliance with the TRM.

Recommendations

We recommend the Chief Information Office:

(1) Ensure interoperability of Composition System Replacement within GPO's Enterprise Architecture and Congress.

(2) Ensure security factors based on a risk-based framework are address before granting an Authorization to Operate.

(3) Evaluate Enterprise Architecture policy and if appropriate revise and implement updated policy to reflect the most recent Federal Enterprise Architecture guidance.

Management's Response

Management concurred with the recommendations. The complete text of management's response is in Appendix C.

Evaluation of Management's Response

We consider the recommendation resolved but will remain open pending our confirmation of the final actions.

Appendix A – Objective, Scope, and Methodology

We performed fieldwork from April through September 2016 at the GPO Central Office in Washington, D.C.

Objective

The objective of our evaluation was to determine the framework GPO followed during development of the CSR system as it pertained to EA.

Scope and Methodology

To accomplish our objective, we—

- Examined relevant Federal EA guidance and GPO policies and procedures.
- Reviewed records associated with system design, development, deployment, testing, and approval.
- Compared relevant guidance, policies, and procedures to activities and processes associated with the design, development, and deployment of CSR in relationship to EA.
- Interviewed key officials performing oversight and approval functions.

Appendix B – Acronyms and Abbreviations

ARB	Architecture Review Board
CIO	Chief Information Officer
CSR	Composition System Replacement
EA	Enterprise Architecture
FDsys	Federal Digital System
FEAF	Federal Enterprise Architecture Framework
GAO	Government Accountability Office
GPO	Government Publishing Office
IT	Information Technology
IV&V	Independent Verification and Validation
OCTO	Office of the Chief Technical Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
TCCB	Technical Configuration Control Board
TRM	Technical Reference Model
XML	Extension Markup Language

Appendix C – Management's Response

ANDREW M. SHERMAN
Chief of Staff

GPO

Date: September 28, 2016

To: Inspector General (IG)

Subj: Draft Report—Organizational Transformation: Composition System Replacement Report Number 16-21

From: Chief of Staff

Thank you for the opportunity to review the subject report. Management concurs with the report's recommendations, as follows:

Recommendation 1: Ensure interoperability of the Composition System Replacement (CSR) project CSR within GPO's enterprise architecture (EA) and Congress.

Response: Concur.

Management agrees that this system should be interoperable within GPO's EA and Congress. Plant Operations and PST have worked with IT throughout the CSR design and development process to ensure interoperability within GPO's EA. Examples of this interaction include:

- The Senior Architect within the IT's Enterprise Architecture Office was an embedded member of the CSR Team for over 12 months. Duties included:
  - Architecture review for all key CSR components.
  - Assistance in selecting key development and architect personnel
  - Hands-on guidance on best practices with respect to system architecture. The design itself built upon previous work executed that evaluated SDL's XML Professional Publisher (XPP) composition engine and coupled it to a GPO EA Created Solution Architecture based upon Microsoft ASP.net technology that is part of the GPO TRM.

- Use of approved technologies and frameworks in accordance with GPO's EA, including:
  - .Net technology stack:
    - C# .Net
    - SQL Server
  - Adherence to IT draft guidelines for Agile Software Development (to be finalized soon)
  - Test-based software development with continuous integration
  - Use of Team Foundation Server for source code and release management
  - Dedicated build server
  - Isolated Development and Test Environments
  - XML Professional Publisher (XPP) as primary composition engine

In addition, the CSR Team (including IT's EA Office) has continuously worked with key staff from the House of Representatives and Senate to ensure that all CSR solutions meet requirements and fit within each environment.

Recommendation 2: Ensure security factors based on a risk-based framework are addressed prior to granting an Authorization to Operate.

Response: Concur.

Plant Operations and GPO's Office of Programs, Strategy, and Technology (PST) are working with IT Security to ensure compliance throughout the process. At present, processes are underway to conduct security reviews for CSR in accordance with GPO IT Security Policy, with the objective of attaining the Authority to Operate for CSR Beta to be delivered in January 2017.

Recommendation 3: Evaluate EA policy and if appropriate revise and implement updated policy to reflect the most recent Federal Enterprise Architecture guidance.

Response: Concur.

GPO EA policy incorporates a modified Federal Enterprise Architecture Framework (FEAF), which has been deemed suitable to GPO as a comparatively small Federal agency within the legislative branch of the Federal Government and compatible with available funding resources. Within these parameters, the CIO and GPO's PST will evaluate GPO's current EA policy and if appropriate revise and implement updated policy to reflect the most recent Federal Enterprise Architecture guidance.

If you need additional information, please do not hesitate to contact me on 2-1100.

ANDREW M. SHERMAN

cc: Director
Deputy Director
General Counsel
Chief Administrative Officer
Chief Information Officer
Managing Director, Plant Operations
Managing Director, Programs, Strategy, and Technoloy

Appendix D - Status of Recommendations

Recommendation	Resolved	Unresolved	Open/ECD*	Closed
1	X		TBD	
2	X		TBD	
3	X		TBD	

*Estimated Completion Date.

Appendix E – Report Distribution

Director, GPO
Deputy Director, GPO
General Counsel
Chief of Staff
Chief Administrative Officer

Major Contributor to the Report

Daniel J. Rose – Lead Information Technology Specialist