U.S. Department of Homeland Security (DHS)
United States Secret Service (USSS)

Integrated Governance, Risk and Compliance (iGRC) Approach

Concept Paper*

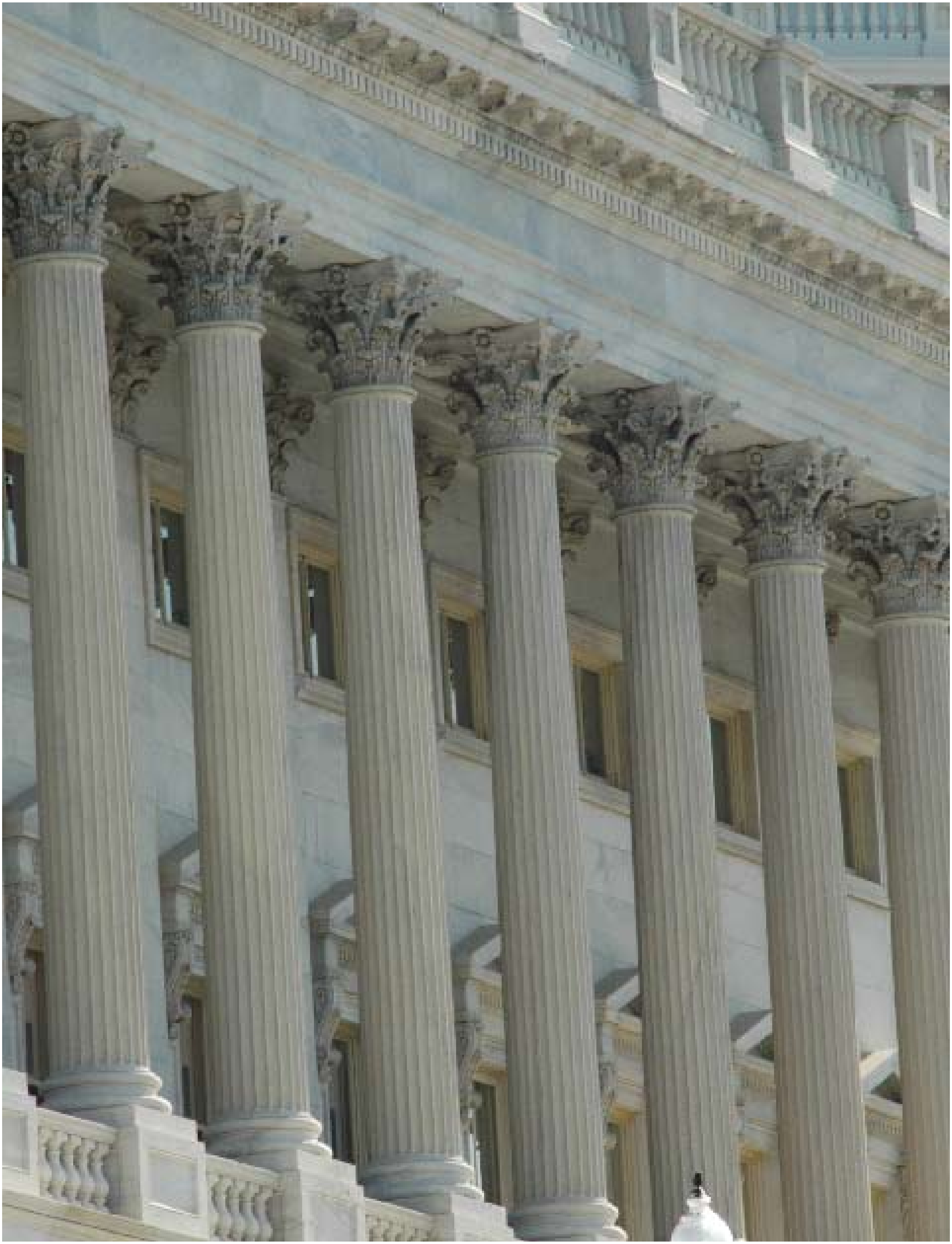
*connectedthinking

PricewaterhouseCoopers

Provided to: Mrs. Nichole Vaughn, Systems Operations Branch Chief
Mr. Steve Vaughn, Systems Integrations Branch Chief
Enterprise Financial Systems (EFS)
United States Secret Service (USSS)
U.S. Department of Homeland Security

Provided by: Jack L. Johnson, Jr.
Principal
1800 Tysons Boulevard
McLean, Virginia 22102
Telephone (703) 918-1303
Fax (813) 329-0173
johnson.jack@us.pwc.com

Table of Contents



Purpose

The purpose of this Concept Paper is to provide the United States Secret Service (USSS) Enterprise Financial Systems (EFS) Branch Chiefs with an integrated Governance, Risk, and Compliance (iGRC) approach to:

1. Test, analyze, and document their Oracle Financials security environment;
2. Link financial and mixed financial system controls, policies, and procedures to applicable laws and regulations; and
3. Procure and configure the Oracle governance, risk, and compliance (GRC) tool.

This iGRC approach will assist the USSS with automating the management of internal controls over business processes, application security, and technical infrastructure security. This iGRC approach will also assist the USSS with improving the efficiency of their compliance processes and complying with applicable laws and regulations.

At USSS specifically, the following IT GRC challenges have been noted:

- Multiple financial and operational information systems that are not centrally managed;
- Lack of available staff resources to ensure compliance with internal control requirements while also supporting the operational and mission needs of the agency;
- Decentralized compliance efforts, which limit the ability to share information and avoid unnecessary work;
- Lack of technology to support documentation, testing, and reporting of compliance activities; and
- High dependence on manual control procedures, with limited use of technology to automate internal controls.

Background

The wide array of complex and overlapping Federal laws and regulations related to the protection of financial information and systems poses a number of challenges to the USSS and EFS Branches. A number of laws have been implemented to protect the confidentiality, integrity, and availability of the sensitive information resources that support Federal operations and assets, including financial systems and data. These laws and regulations include the Federal Information Security Management Act (FISMA) of 2002, the Federal Managers' Financial Integrity Act (FMFIA) of 1982, and the Federal Financial Management Improvement Act (FFMIA) of 1996.

FISMA requires each Federal agency to develop, document, and implement an entity-wide security program to protect the information and information systems that support the operations and assets of the agency, including both financial and non-financial systems and data. FMFIA provides additional requirements specific to systems supporting financial accounting and reporting, including Chief Financial Officer (CFO)-Designated Financial Systems. FFMIA requires that Federal financial management systems comply with Federal systems requirements and accounting standards, and that they also comply with the U.S. Standard General Ledger at the transaction level. Specific guidelines for addressing the laws and regulations are included in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 and OMB Circular A-130, which are applicable to all IT systems, and OMB Circulars A-123 and A-127, which are applicable to significant financial system internal controls. In addition, the Department of Homeland Security (DHS) Financial Accountability Act (DHS FAA) requires DHS Management to provide an assertion on internal controls over financial reporting (ICOFR) and to obtain an independent audit opinion on ICOFR.

In October 2007, the DHS issued updates to DHS Sensitive Systems Policy Directive 4300A and the DHS 4300A Sensitive Systems Handbook with additional guidance for the Department's financial systems. DHS 4300A requires the DHS Chief Information Officer (CIO) to establish and oversee the Department-wide IT Security Program, and it includes specific requirements for the DHS CFO related to the Department's financial systems. In addition, DHS 4300A requires the components to (1) conduct annual assessments of the design and operational effectiveness of 27 key A-123 ITGCs and (2) monitor or maintain documentation evidencing the effectiveness of key security-related controls. These requirements build upon DHS's existing FISMA/NIST 800-53-based IT security and control framework, which includes a compliance review program that incorporates an evaluation of the security documents uploaded into the Department's Trusted AgentFISMA (TAF) tool, as well as on-site evaluations of a sample of DHS systems.

The USSS and other Federal agencies continue to be challenged by this array of applicable laws and regulations, particularly as they relate to developing, implementing, maintaining, and enforcing consistent financial policies and procedures. As Figure 1 illustrates, the effort required to achieve compliance with applicable laws and regulations may lead to assessment fatigue, duplicative data, gaps in risk activities, overlapping efforts, inconsistent processes, and unclear roles and responsibilities.

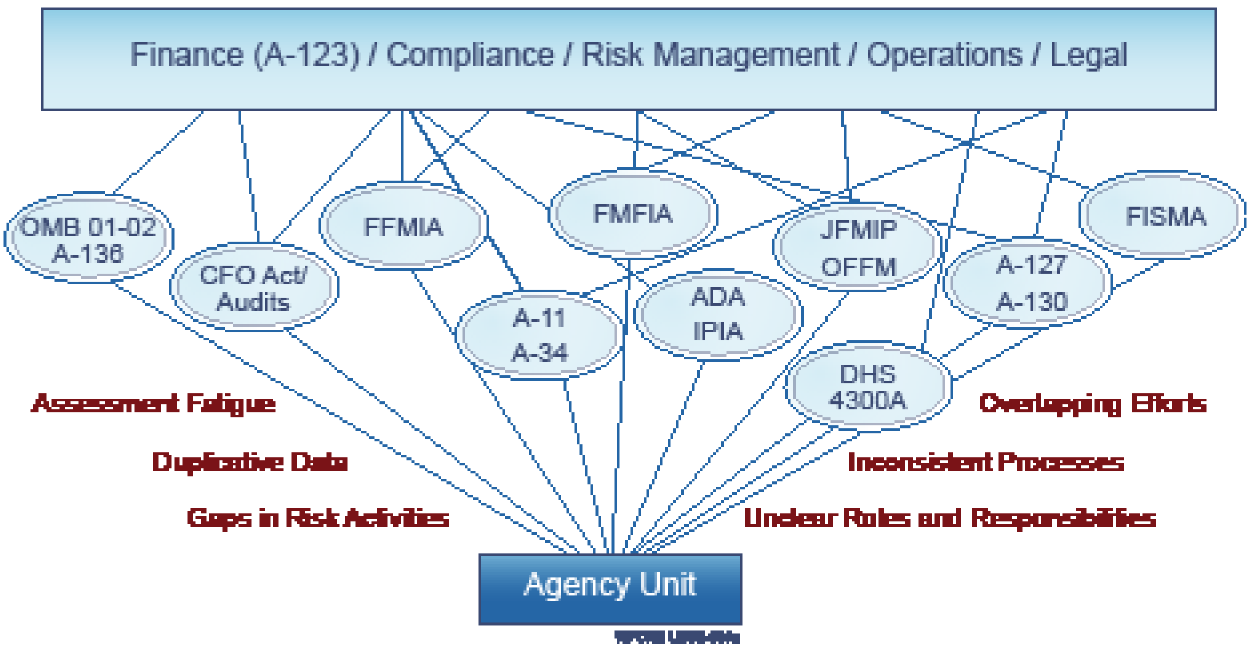


Figure 1: Opportunities for integration of the Oracle governance, risk and compliance tool.

To address these IT GRC challenges, the USSS may consider opportunities for integration of the Oracle GRC tool. GRC tools automate the management of internal controls over business processes, application security, and technical infrastructure security. GRC tools will also assist the USSS improve the efficiency of their compliance processes and comply with applicable laws and regulations. The USSS is currently in the process of evaluating the Oracle GRC tool, which carries out a range of functions such as:

Documentation of Policies and Procedures

- Creates a central repository to store and manage content for all GRC initiatives (including documentation created by the DHS Internal Control Program Management Office to be used by all DHS components), giving users a single view and access point to critical information, including policies and procedures, process diagrams, control descriptions, test plans, control matrices, and remediation plans for issues; and,
- Automates the creation, approval (including periodic reviews), distribution, editing, and archiving of policies and procedure documents; and

Continuous Monitoring of Controls

- Monitors user access/segregation of duties (integrated workflow and approvals) and provides internal automated controls reporting;
- Creates dashboards for controllers, auditors, and business process owners so that users can quickly construct their own reports for on-the-spot analysis;
- Tracks risk metrics and thresholds, triggering an alert/notification to appropriate personnel when thresholds are breached (integrated workflow and notification); and
- Utilizes date-effective audit trails that track “who, what, and when” changes made to risk-control matrices, work papers, and other documentation.

Enforcement of Policies and Procedures

- Enforces user access/segregation of duties; and
- Delivers policy education via online, self-paced learning with the user interface optimized for training (creates tests to assess employee understanding and to provide feedback on policy design).

See Figure 2 below for the Oracle GRC processes.

If implemented appropriately, use of the Oracle GRC tool will help the USSS automate the management of internal controls over business processes, application security, and technical infrastructure security via the following approach:

- Testing, analyzing, and documenting the Oracle Financials security environment to identify the USSS Oracle security baseline;
- Linking financial and mixed financial system controls, policies, and procedures to applicable laws and regulations;
- Evaluating and implementing the Oracle GRC tool best suited for the USSS environment;
- Configuring the Oracle governance, risk, and compliance tool to meet the USSS' needs to help automate internal controls over business processes, application security, and technical infrastructure security. This would typically include workshops and interactive client sessions to define and collect tool requirements; and
- Conducting testing, remediation, and training activities to maintain the effectiveness of the tool.

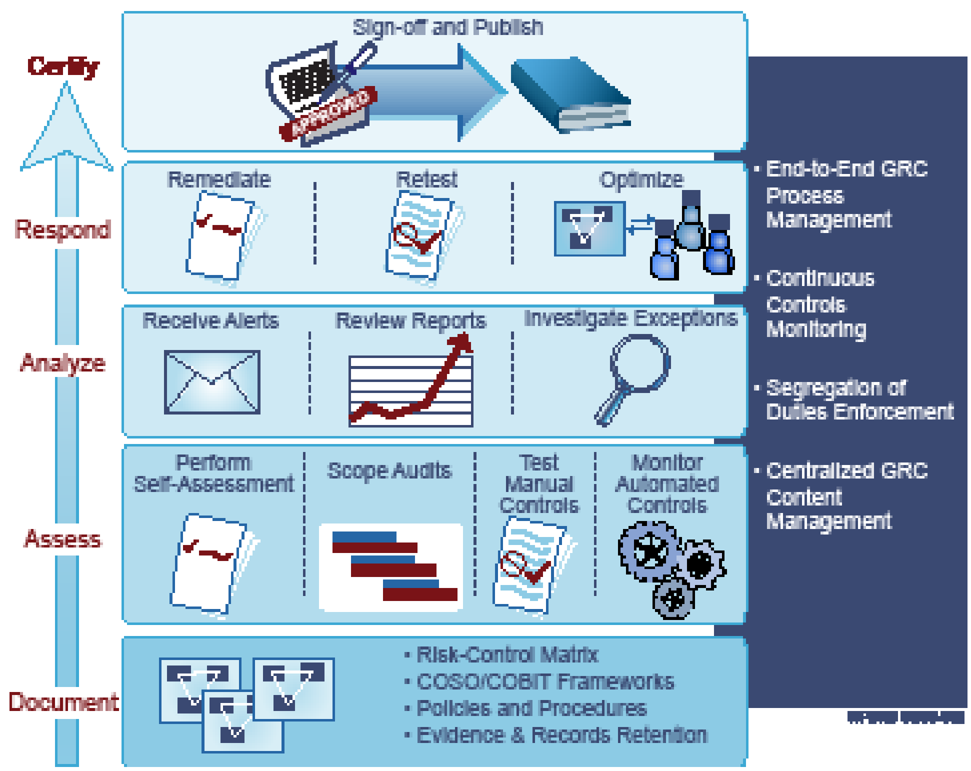


Figure 2: Oracle GRC Processes.

Approach

Integrated GRC Approach Summary

The USSS EFS Branch Chiefs may consider a three-phased approach to implementing the Oracle GRC tool that would ensure IT security controls are identified via walkthroughs and assessments, mapped to applicable laws and regulations, and integrated into the GRC tool by building the requirements. This integrated GRC approach would consist of the following activities:

- Assessing Oracle Financials security and control configurations for specific modules and supporting infrastructure. This assessment can help the USSS establish the Oracle security baseline, identify control weaknesses, and develop achievable remediation actions. The results of this assessment can be leveraged to link key controls to applicable laws/regulations and control weaknesses.

- Mapping the USSS technical, operational, and management controls (as defined in DHS 4300A) for financial and mixed financial systems to the applicable laws and regulations identified in Figure 1. The USSS may also consider addressing compliance with DHS policies and procedures in this mapping exercise. Gaps in IT documentation, compliance and/or security control requirements can be identified and remediated.

- Identifying GRC tool requirements, conducting the vendor selection process, implementing the tool, and integrating it within the USSS. This includes customizing the GRC tool to the USSS needs, including workshops and interactive client sessions to define and collect tool requirements.

Oracle Financials Assessment

In order to effectively map the USSS policies, procedures, and other manual/automated controls to applicable laws/regulations in preparation for a GRC implementation, the USSS may consider identifying its Oracle security baseline. This can be achieved by performing a security and controls assessment of Oracle Financials for specific modules and supporting infrastructure. The review can use a risk-based methodology to assess the following:

- Oracle Application Security: assessing the creation and assignment of Oracle Responsibilities (application security profiles) for proper segregation of duties. This includes sampling Oracle Responsibilities and users to ensure that excess privileges have not been granted;

- Business Process and Manual Controls: Assessing the adequacy of the business process and manual controls that support the application (i.e., monitoring controls);

- System Administration: Assessing the controls around the administering of user IDs and passwords, system auditing, and user monitoring procedures;

- Oracle Database: Assessing the security and controls over the database; and,

- Operating System: Assessing the security and controls over the operating system.

Mapping the USSS Technical, Operational, and Management Controls

The USSS may consider mapping its IT policies, procedures, and other manual/automated controls to applicable laws and regulations identified in Figure 1. The USSS may also include compliance with DHS policies and procedures in this mapping. This will help the USSS to:

- Determine what overlap exists between apparently differing applicable laws/regulations and perform cost/benefit analysis of addressing control gaps;
- Respond to various regulators and auditor requests more quickly to avoid duplication of efforts; and,
- Evaluate risk exposure across the enterprise.

GRC Tool Implementation and Training

GRC tools allow management to access relevant compliance and governance information, and examine how internal controls over business processes, application security, and technical infrastructure security are implemented. In order to identify and implement GRC tool requirements, the USSS may be able to utilize the mapping results (see Mapping the USSS Technical, Operational, and Management Controls) and output from the Oracle Financials Review (see Oracle Financials Assessment section) to perform the following actions:

- Identify business rules and internal controls over financial reporting (including business processes, application security, and technical infrastructure security) which will be included in the system requirements;
- Identify user access privileges and segregation of duties requirements which will be included in the system requirements; and,
- Document, test, and sustain the business rules, internal controls over financial reporting (including business processes, application security, and technical infrastructure security) and access privileges over time to achieve audit readiness and A-123 compliance.

The USSS may also consider conducting testing, remediation, and training activities to maintain the effectiveness of the tool.

Project Milestones

The USSS EFS Branch Chiefs may consider the following milestones for addressing the aforementioned objectives:

Short Term:

- Begin to identify GRC tool requirements and continue to conduct the vendor selection process.

- Perform a security and controls assessment of Oracle Financials for specific modules and supporting infrastructure. Completing this assessment will allow the USSS to proactively document current IT controls and analyze the root causes for noted control weaknesses. Based on the results of this assessment, the USSS should update its Plan of Actions and Milestones (POA&Ms), as necessary, to remediate root causes.

Intermediate Term:

- Map the USSS technical, operational, and management controls for financial and mixed financial systems to the applicable laws and regulations identified in Figure 1. The USSS should also include compliance with DHS policies and procedures in this mapping. Perform gap analysis to identify gaps in IT documentation, compliance and/or security control requirements.

- Finalize and implement updated IT controls policies and procedures that align to DHS security requirements based on the Oracle Financials assessment and IT documentation gap analysis.

- Utilize the results of the Oracle Financials assessment and gap analysis to report results for compliance with applicable laws and regulations identified in Figure 1, including A-123 compliance. The results should also be leveraged for building requirements for the GRC tool.

- Procure the GRC tool and install it into the USSS environment.

- Configure the governance, risk, and compliance tool to the USSS' needs, which typically include workshops and interactive client sessions to define and collect tool requirements.

Long Term:

- On a periodic basis, evaluate the operational effectiveness of IT security controls over financial and mixed financial systems and implement compensating controls to reduce risks, while developing overall long-term, sustainable solutions.

- Monitor and report compliance with the USSS security policies and procedures.

- Continue to customize the GRC tool to the USSS' needs, hosting remediation workshops and interactive client sessions to define, collect, and modify tool requirements.

- Conduct testing, remediation, and training activities to maintain the effectiveness of the tool.

Contractor Deliverables

For a specific time period, the USSS may require the contractor to provide the following deliverables:

- Reports detailing the IT controls in place and control design weaknesses identified for IT Oracle Financials assessments (see Oracle Financials Assessment section for specific reviews that may be conducted and documented).
- Matrices detailing the result of the mapping of the USSS controls to applicable laws and regulations. This may include a gap analysis of the USSS IT documentation and compliance with applicable laws/regulations and DHS requirements. This gap analysis may also include suggestions for enhancing current policies, procedures, technical controls, and practices, as well as new documentation that may need to be developed, implemented, and communicated.
- Requirements documentation, utilizing the Oracle Financial assessment results and mapping matrices, which helps to build the IT controls within the GRC tool.
- Biweekly status reports that include the following information:
    - Progress of the three work streams (Oracle Financials Assessment, Mapping Matrices, and Requirements Documentation);
    - Project budget analysis;
    - Any project issues; and,
    - Accomplishments and next steps.

Informally, the contractor may provide the USSS EFS Branch Chiefs with any additional draft documentation or output that may be created at management's request to assist the USSS with the implementation of the GRC tool.

Required Support Capabilities

Choosing the right support is crucial to the USSS' ability to integrate the GRC tool into its environment. Choice of support should be based on experience and technical know-how. Specifically, the USSS external support team should have the following capabilities:

- Ability to begin Oracle Financials assessment, mapping efforts, and GRC support immediately;
- Experience with the USSS IT environment and performing tests of design and operating effectiveness for internal controls over financial reporting for the USSS;
- Specific prior experience with and a significant understanding of the USSS IT infrastructure, including both major applications and general support systems;
- Experience with performing Oracle assessments / reviews worldwide;
- Experience with unique issues surrounding Oracle assessments, implementations, upgrades and redesigns;
- Experience in helping companies maximize the return on their investment in Oracle through the application of effective and efficient internal controls;
- Experience in assisting with the selection, implementation and integration of business processes with GRC tools;
- Experience with the DHS Office of Chief Information Officer's 27 key information technology general controls that are part of the DHS OMB A-123 Appendix A Compliance Framework requirements;
- Experience in performing audits of internal controls over financial reporting in the Federal Government, and issuing an Opinion on Internal Controls in the Federal Government;
- Experience in performing tests of design and tests of operating effectiveness for internal controls over financial reporting for the Department of Homeland Security;
- Experience in developing and implementing strategies for remediation of weaknesses in internal controls in accordance with the Department of Homeland Security Corrective Action Planning guidance;
- Experience with the GAO Federal Information System Controls Audit Manual (FISCAM), FISMA/National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Federal financial statement audits, and Federal internal controls improvement initiatives;
- Demonstrated understanding of USSS Chief Information Officer (CIO), Chief Financial Officer (CFO), Information Resource Management Division (IRMD), and EFS mission and objectives.
- At least five (5) years of sustained experience executing large support efforts specifically related to eDiscovery and Electronically Stored Information (ESI);
- Domestic capacity, capability, and experience to conduct enterprise information technology infrastructure assessments;
- Experience preserving and analyzing large volumes of structured and unstructured ESI in support of mission objectives;
- Demonstrated ability to use the USSS' sophisticated eDiscovery data-mining tools to support mission objectives;
- Ability to determine functional and technical requirements to assist with a rapid deployment of a scaleable and secure web based electronic document review applications;
- Ability to deploy resources throughout the United States;
- Recognized Project Management Methodology to run large, complex engagements; and,
- Experienced and cleared computer forensics specialists and staff who have a deep understanding of the USSS IT infrastructure and possess the following certifications:
    - Certified Public Accountants (CPA);
    - Certified Information System Auditors (CISA);
    - Certified Information Systems Security Professional (CISSP);
    - Certified Fraud Examiners (CFE);
    - EnCase Certified Examiner (EnCE); and
    - Certified Project Management Professional (PMP).

pwc.com