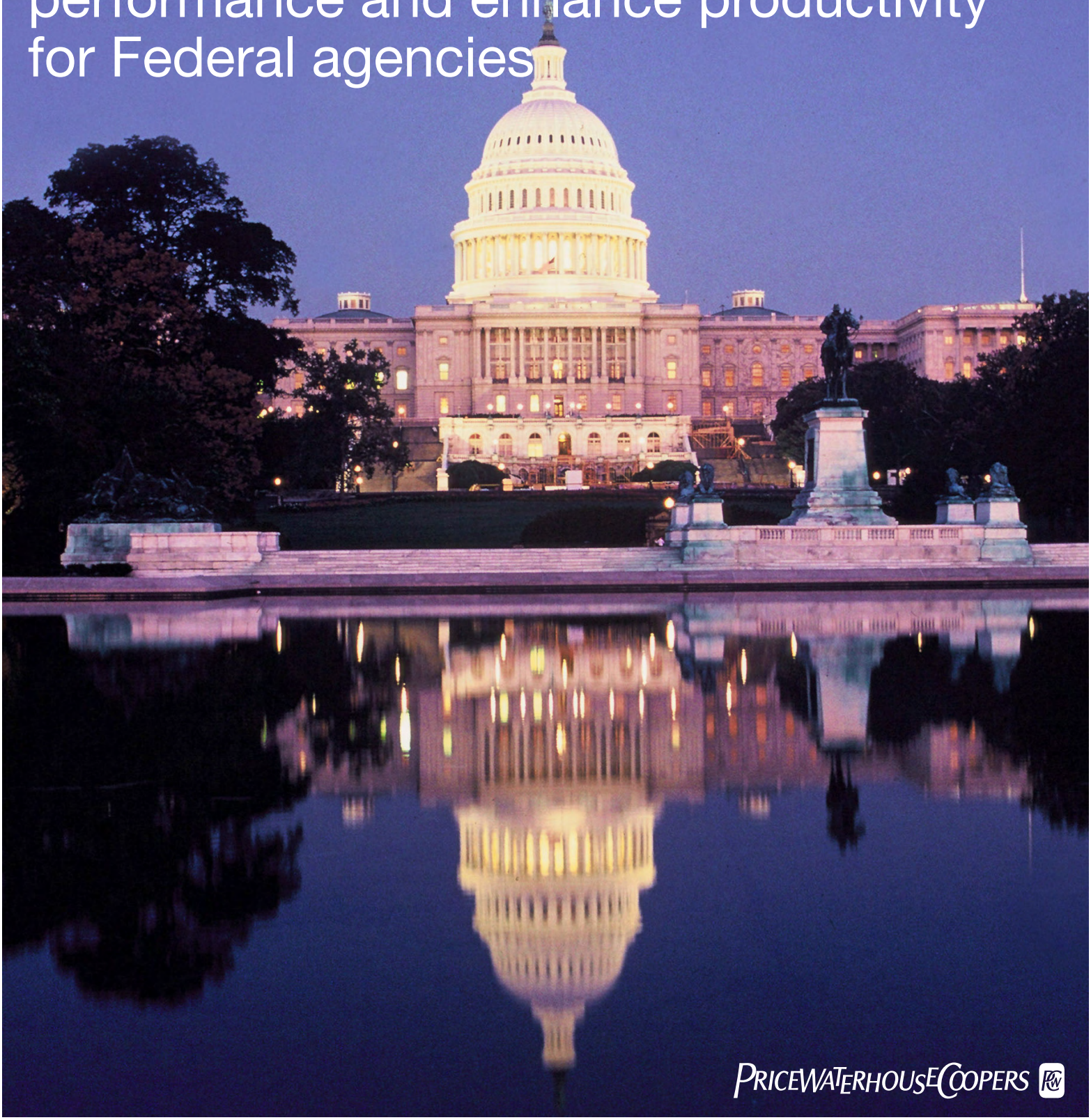
Integrated Governance Risk and Compliance

How the right approach can improve performance and enhance productivity for Federal agencies



PricewaterhouseCoopers

For further information, please contact:

Scott R. McIntyre
Principal
scott.mcintyre@us.pwc.com
(703) 918-1352

Christopher Stansbury
Managing Director
christopher.stansbury@us.pwc.com
(703) 918-1045

Gregory Williams
Director
gregory.s.williams@us.pwc.com
(703) 918-1517

Table of Contents

Introduction

In recent years, high profile accounting and management scandals in the commercial sector have given rise to legislative action to improve internal controls over financial reporting for companies participating in the financial markets. The Sarbanes-Oxley Act of 2002 is the most recognizable of these initiatives, and it held implications for both public and private institutions to improve oversight for financial management and reporting. Additional laws and regulations have been passed since outlining requirements for establishing and maintaining internal controls for Federal agencies, the most notable of these being the Office of Management and Budget's (OMB) Circular A-123. In December of 2004, OMB updated Circular A-123 with Appendix A to prescribe a strengthened process to assess the effectiveness of the internal controls over financial reporting for CFO Act agencies.

Since the release of Appendix A, many Federal agencies have undertaken a comprehensive review of their internal control environments to validate compliance with the requirements, identify control gaps or deficiencies, and define and implement remediation activities based on the findings. These reviews have uncovered a general need across the federal government to improve internal controls over financial reporting, including organizational, process, and technology related controls. These improvements are necessary to enhance an agency's fiduciary responsibility over their assets, as well as to bolster the validity of financial statement assertions. Perhaps more importantly however is that these improvements can and should also lead to improved process performance and productivity. PricewaterhouseCoopers' (PwC) approach therefore, goes beyond the compliance exercise to provide a comprehensive approach for business process improvement (BPI) for Federal agencies.

PwC has supported hundreds of organizations in both the commercial and Federal sectors through internal control reviews and subsequent remediation efforts to improve their control environments. Notable agencies where we have performed A-123 reviews for example, include the Department of Homeland Security (DHS), Department of the Interior (DoI), and the Federal Bureau of Investigation (FBI). Through our experience, PwC has identified a set of common critical factors that agencies should consider in establishing a robust and comprehensive internal control program, which are further described in the bullets to the right.

The remainder of this document outlines a proposed approach that brings together PwC's substantial audit experience, knowledge of specific compliance challenges facing Federal agencies, and our experience with key enabling technologies to provide a clear roadmap for meeting the compliance challenge and implementing business process improvements. This approach, known as Integrated Governance, Risk and Compliance (iGRC) provides a principles-based approach to making compliance an integrated part of an agency's way of doing business.

GRC lessons learned:

- **Government organizations must understand the universe of applicable compliance and internal control requirements and their interrelationships.** Given the scope and complexity of policies, laws and regulations that must be analyzed and implemented, agencies must be equipped with resources who have helped organizations achieve compliance. This experience should include not only knowledge of regulatory requirements, but an auditor's perspective to fully understand internal control compliance both from a risk standpoint, as well as the related impact to financial statement assertions.

- **Government agencies should apply an integrated approach to governance, risk, and compliance to prevent duplication of activities.** The establishment of proper internal controls should not be a separate or "stand alone" compliance activity, but rather a core element of an agency's routine operations. Organizations that embed robust internal controls across organizational, process and technology boundaries are most successful in achieving both compliance and improved business process performance.

- **Agencies should leverage information technology tools to improve the efficiency of documentation, testing, and the actual functioning of internal controls.** Technology has evolved as a reliable, efficient and critical enabler to help agencies manage complex compliance requirements. Much like their commercial counterparts, government agencies are using Governance Risk and Compliance tools to not only help structure and document their review programs, but also to automate preventative controls such as managing the segregation of duties within the core financial system. Previous experience integrating these tools into an agency's overall compliance process is key to maximizing the return on this investment.

Compliance Challenges Facing Federal Agencies

While the Federal Managers' Financial Integrity Act (FMFIA) has been in place since 1992, OMB Circular A-123 (Appendix A), which defines management's responsibility for internal control, was revised in 2004 to provide further clarity on relevant internal control requirements for CFO Act agencies.

The revisions to OMB Circular A-123 (Appendix A) and the level of effort required for compliance have gathered a significant level of attention across Federal agencies. However, as shown in Figure 1, there are a number of additional internal control and security related laws and requirements that are equally challenging and important. These include, but are not limited to:

- The Budget and Accounting Procedures Act of 1950
- The Inspector General Act of 1978
- The CFO Act of 1990
- Federal Financial Management Improvement Act of 1996
- Federal Information Security Management Act of 2002

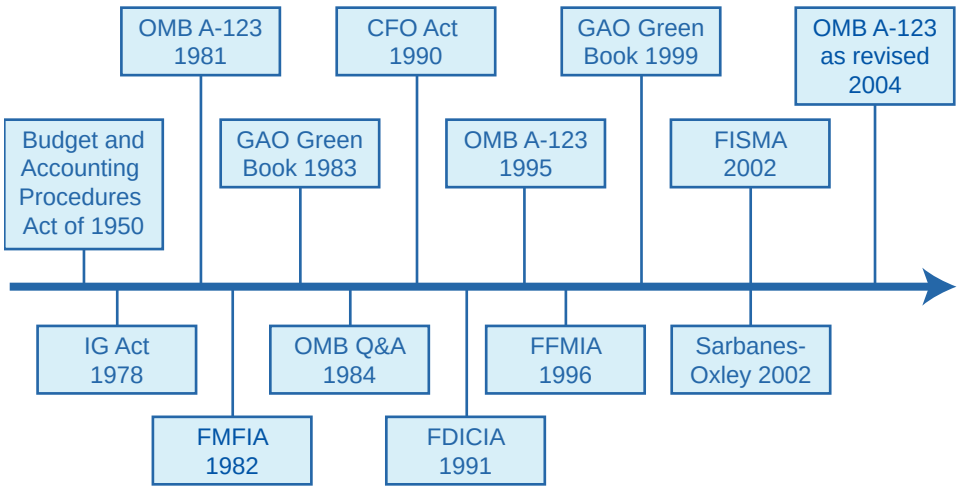


Figure 1: Federal Laws/Regulations Impacting Compliance.

What is Internal Control and What is Required?

The GAO Standards for Internal Control in the Federal Government (often referred to as the Green Book), detailed in Figure 2, provides the following definition of internal control: "Internal control…..comprises the plans, methods, and procedures used to meet missions, goals, and objectives…. and provides reasonable assurance that the following objectives (depicted in Figure 2) are achieved."

OMB Circular A-123 (Appendix A) provides additional clarity and defines internal control over financial reporting as a process designed to provide reasonable assurance regarding the reliability of financial reporting, and also states internal control over financial reporting should:

- Assure the safeguarding of assets from waste, loss, unauthorized use, or misappropriation; as well as
- Assure compliance with laws and regulations pertaining to financial reporting.

OMB Circular A-123 (Appendix A) also provides guidance on requirements for agency management regarding internal controls over financial reporting. At a high level, these requirements include:

- Agency heads **annually evaluate and report** on the control and financial systems that protect the integrity of Federal programs
- Agency heads **must issue an 'Annual Statement of Assurance'** on overall adequacy and effectiveness of internal control within the agency.

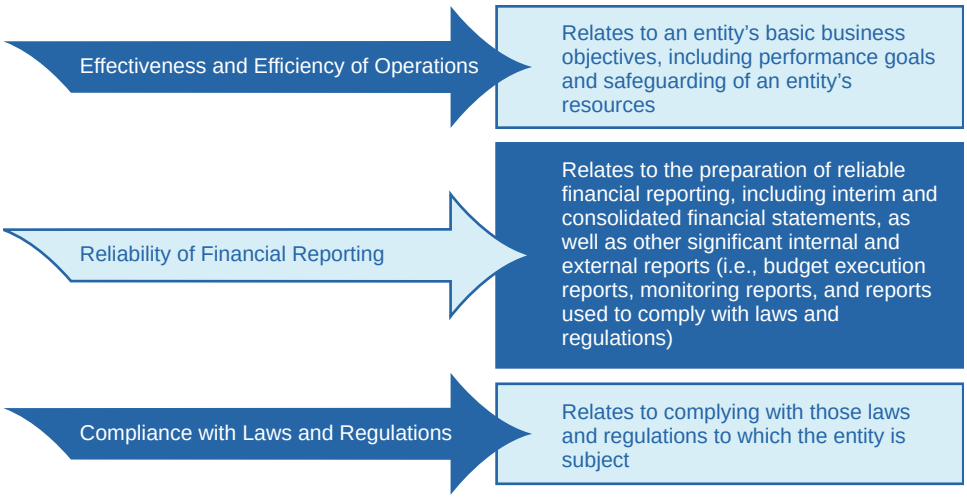


Figure 2: Internal Control Objectives.

The Challenges/Lessons Learned

Each individual legal and regulatory requirement is complex and requires significant organizational planning and effort to achieve compliance. The challenge Federal agencies face is exacerbated by a number of factors:

- Large geographically disbursed organizations with varying missions
- Decentralized management responsibility for component organizations
- Multiple financial and operational information systems that may not be centrally managed
- Lack of available personnel to focus on internal control requirements and complete the operational mission of the agency
- Compliance efforts may be decentralized, limiting the ability to share information and avoid unnecessary re-work
- Lack of technology to support documentation, testing, and reporting of compliance activities
- High dependence on manual control procedures with limited use of technology to automate internal controls.

The organizational, process, and technology challenges facing those responsible for ensuring and asserting the adequacy of internal controls in the Federal Government can be formidable. However, there are a number of lessons and best practices that can be taken both from the commercial world and from Federal agencies that have proactively addressed the requirements of Sarbanes-Oxley and OMB Circular A-123. Most notable among these lessons and best practices are:

- Implementing a risk-based approach to focus on the essential elements
- Centralizing internal controls documentation development, maintenance, and testing
- Adopting a program management approach to internal controls and compliance
- Understanding and leveraging the organization's efforts towards disparate compliance and internal control requirements, thereby minimizing the need for repetitive activities
- Utilizing, to the maximum extent possible, the inherent and configurable automated controls within legacy and COTS applications to enforce controls over transaction processing
- Minimizing reliance on manual controls and decentralized responsibility for compliance activities that are difficult to sustain over time.

Accelerating the Process via Governance Risk and Compliance (GRC)

One of the key success factors in achieving both short- and long-term success is approaching compliance and internal controls in an organized and controlled manner. Often the work performed relating to internal controls over financial reporting supports higher-level organizational Governance, Risk, and Compliance (GRC) objectives. GRC can be defined as the organization's practices and the various roles that senior management, line management, and the rest of the organization play with respect to compliance with laws and regulations and internal policies and procedures. To understand the interrelationships between governance, risk management and compliance (GRC), their meaning and scope must first be understood. PwC defines them as follows:

- **Governance:** The process and structure used to direct and manage the business and affairs of an agency with the goal of promoting its financial viability. Equally important, it encompasses the impact of key strategic decisions on all stakeholders, from regulators and employees to customers, suppliers and the public. Its activities generally focus on developing policies, objectives, and planning strategy.
- **Risk Management:** A comprehensive, systematic approach for helping agencies, regardless of size or mission, identify events and respond to the risks challenging its most critical objectives and related projects, initiatives, and day-to-day operating practices. Risk management deals with determining the agency's risk appetite, and then identifying and mitigating risks to appropriately balance the risk portfolio.
- **Compliance:** A desired outcome, with regard to laws and regulations, internal policies and procedures, and commitments to stakeholders that can be consistently achieved through managed investment of time and resources. Compliance management includes the legal and tactical activities in day-to-day business processes.

Figure 3 illustrates the silos of activity of each GRC discipline and some of the activities that occur in each. As these silos are established, the relationships between the practices become clearer.

A lack of GRC coordination creates inconsistencies or redundancies in control activities and increases overall costs. It is true that each discipline is important in its own right but GRC vendors, leading analyst firms, and business consultants all recognize that governance, risk, and compliance must function interdependently as part of an integrated strategy. Only with an organizational view of GRC information and a unified solution for managing GRC across the enterprise can organizations manage with confidence, improve business predictability, and drive higher performance.

Most Federal agencies today have established positive momentum in solving the complexity in interactions, ineffective risk management, and inefficient compliance. However, the approach to integrating governance risk and compliance activities remains fragmented in four key areas:

- **Organizational Fragmentation:** Organizationally, the identification of risks, implementing policies, identifying and measuring risks, and supporting regulatory mandates takes place at the departmental level. Disconnected departmental activities can result in inconsistent policies, difficulty predicting risk, duplication of effort, and a lack of enterprise transparency. The consequences of organizational fragmentation intensify and risk increases when collaboration with partners and suppliers increases. The organization is then held responsible for good governance and compliance within the confines of its own enterprise and across the extended enterprise.

- **Systems Fragmentation:** Information about governing principles and policies, risk measurement, and compliance with regulatory mandates are still supported by departmental IT systems, making the aggregation of data a complex and time-consuming task. Local process optimization and implementation of point solutions can further isolate information within systems, resulting in a lack of information integrity and a limited view of enterprise risk.

- **Regional Fragmentation:** Policies and risks are generally defined and measured at the local level, without proper consideration of their impact on the global, multinational, national, or regional mandates with which an agency must also comply. Decision makers are often unaware of the interdependencies of various mandates, and of the risks associated with the multitude of jurisdictions, countries, and markets in which they conduct business. As a result, agencies may suffer tangible (financial) and intangible (brand and reputation) consequences.

- **Increasing Numbers of GRC Initiatives:** The ever-increasing number of governance, risk, and compliance initiatives exacerbates fragmentation. Horizontal mandates address such areas as financial reporting, security, privacy, records retention issues, import-export regulations, environmental standards, occupational safety, and credit risk exposure involving all types of businesses. Vertical mandates additionally address an exhaustive number of industry-specific areas. Without an aligned and integrated perspective on governance to guide risk profiling and mitigation, organizations cannot effectively monitor compliance and risk, nor can they adjust business processes to meet changing requirements, market trends, and regulatory mandates, thus optimizing risk/return portfolios.

The current challenges are to document the control environment, test automated and manual business processes, resolve exceptions, report financial results, and optimize business processes. The question is how to build value from this recent momentum so that governance, risk, and compliance function interdependently as part of an integrated strategy.

Governance	Risk Management	Compliance Management
• Establish qualitative objectives • Establish quantitative objectives and KPIs • Develop strategies to achieve objectives • Document corporate policies and best practices standards • Review and measure progress toward objectives • Review financial results, auditor reports, legal issues • Investigate whistle-blower claims • Establish remuneration for key management	• Identify risks and opportunity costs: market, legal, operations, environmental, financial, etc. • Identify relationships between risks • Determine risk appetite, select risk treatment options, and allocate investments and resources accordingly • Implement risk management methodologies, frameworks, calculation models, KPIs, and tolerance thresholds • Collaboratively measure risk impact and probability • Periodically review and reassess risk profile • Monitor for key events and assess impact on risk profile	• Identify compliance requirements: regulatory, organizational policies, etc. • Select compliance frameworks • Document and implement business processes and controls • Identify and address control gaps • Monitor control effectiveness and status • Remediate control issues • Periodically review and update control environment • Certify control effectiveness • Analyze and report results to key audiences • Generate body of evidence to support auditor requirements • Assess impact of key events on controls

Figure 3: GRC Activities.


CONSTITUTION AVE NW
1000

Addressing the GRG Challenge: PwC's iGRG Methology

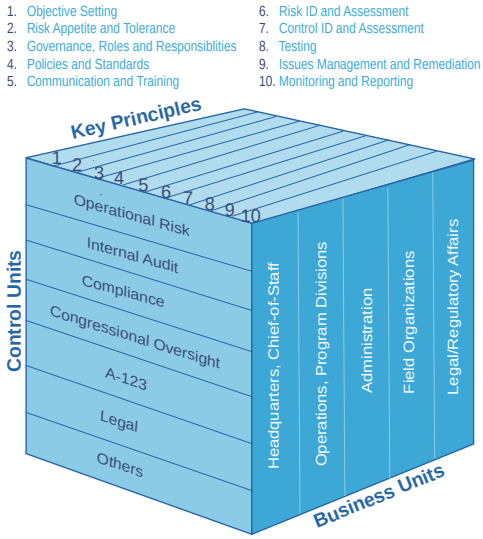


Figure 4: Key Principles, Control Units, and Business Units.

PwC's integrated GRC (iGRC) approach uses a principles-based framework to help identify integration gaps and target opportunities for enhancement. For almost any organization, there is a set of common governance, risk and compliance activities that are executed across business units and control functions. These core activities are referred to as principles. PwC has categorized and combined the 110 Committee of Sponsoring Organizations of the Treadway Commission (COSO) principles into 10 key principle categories, as shown in Figure 4. Control units are the functional areas that manage governance, risk, and compliance activities. The enablers – people, process, technology, and information – are known as levers.

Levers are located at the intersection of principles, control units, and business units that perform various governance, risk, and compliance activities. The relevant standards and regulatory requirements can be identified based on the functions and activities across risk-related corporate governance functions. Industry-accepted standards can be tailored, as appropriate, based on the scope and objectives of the analysis, into principles for evaluation. Finally, target principles are analyzed through the four operating levers that are used to perform activities.

Based on a generally accepted GRC-principles taxonomy and four enabling levers – people, process, information, and technology – our four-step methodology establishes a unified framework for identifying common components across control units to form a basis for integration. In the Assessment phase, we assess the compliance requirements and business processes across the enterprise to identify potential points of integration, the criteria for evaluating compliance activities, management's risk appetite, compliance risks, and management's priorities for compliance improvements. During the Control Unit Integration phase, we identify specific improvement actions, develop a business case for change, determine implementation strategies, plan change management activities, and develop metrics. In the Business Unit Integration phase, we complete changes to the compliance operating model, technology, organization, and internal controls. We also define roles and procedures, and develop communications and training plans. Finally, in the Operational Implementation phase, we roll out process, technology, organizational structure and controls changes, and train personnel in the controls architecture. We implement monitoring, reporting, and exception handling processes to ensure that change initiative goals are monitored and maintained, and that continuous improvement plans are realized.

As can be seen, the foundation of our four step methodology is to use compliance as a key driver for achieving business process improvement. This concept was developed through our work performing numerous A-123 studies where we recognized that our recommendations to remediate control weaknesses have led to agencies implementing improvements that have not complicated, but actually enhanced business operations while at the same time reducing the risk of loss (e.g., monetary, reputational, security, etc.). Through this experience, we can better advise our Federal clients on business process improvement strategies that convey both compliance and enhanced productivity.

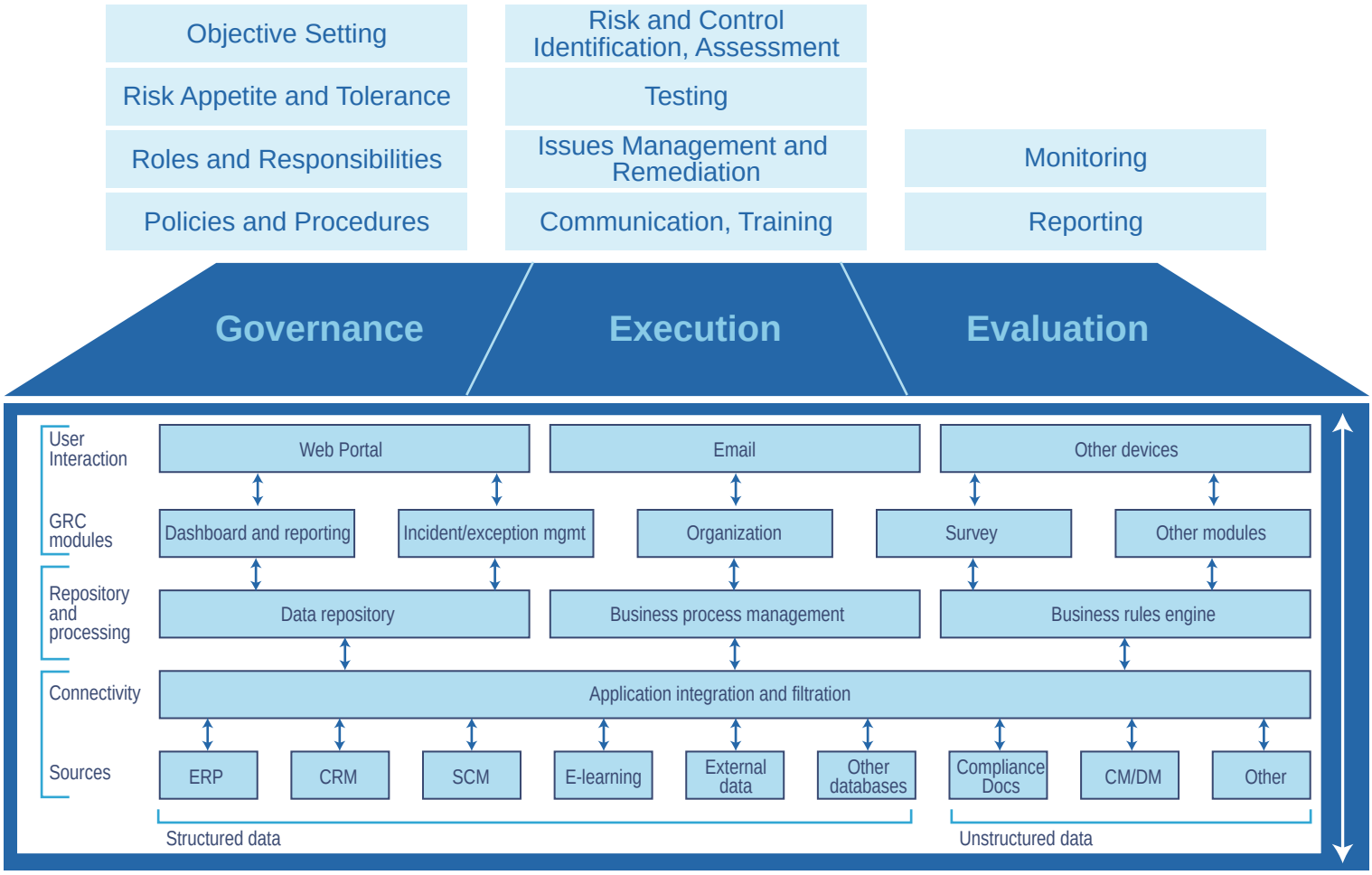


Figure 5: iGRC Functional Architecture.

Leveraging Technology to Streamline GRC Initiatives

Using PwC's iGRC principles-based approach, the technology lever provides a structured means, or architecture, to streamline and consolidate, standardize, and communicate governance, risk, and compliance information. Technology components, such as repositories of business processes, control and risk information, security, networking, and business intelligence help determine which solutions best map to the iGRC principles and the needs of the agency. PwC's functional architecture, shown in Figure 5 above, provides an integrated view of managing the information flow among the technology components, and interaction with the organization and related processes and common data elements.

The architecture above is realized by leveraging various types of technology capabilities to include the following:

- **Discrete Solutions –** Specific risk and compliance processes that have targeted software solutions (e.g., document management, change control software, etc.). These solutions address specific risk and compliance requirements, but also need to be integrated into a larger framework/ architecture.
- **Optimized/Extended Use of Current Technology –** The leveraging of existing in-house systems, extending the functionality of those systems and/or improving the data quality of the information in existing systems (e.g., fully leveraging the controls built into an ERP package).
- **Real-time Risk and Compliance Environment –** Leveraging investments across discrete solutions and in-house applications utilized with real-time integration technologies to establish a real-time GRC environment. Newer technologies and techniques, such as service-oriented architectures, web

Principles	Examples of COTS Capabilities Provided
Objective setting	Database and content management technologies provide a way to centrally manage and communicate GRC information across the enterprise. They also provide an audit trail and documentation in support of compliance and risk management.
Roles and responsibilities	Security solutions including Identity Management and Roles Based Access Control software provide a master list of control owners to highlight accountabilities, enforce Segregation of Duties, and guide workflow and approvals.
Policies and procedures	Policy management solutions automate the creation, approval, and maintenance of GRC policy and procedure documents. Automation also helps with the correlation of policies to regulatory requirements.
Risk and control identification and assessment	Risk management solutions track risk metrics and thresholds, triggering a notification when thresholds are breached. Control management solutions automate the deployment and monitoring of controls for both business processes and IT infrastructure to ensure compliance with financial reporting regulations and other frameworks (e.g., GLBA, PCI, COBIT).
Testing	Provides central repository of test plans. Deploy the same automated control test across multiple organizations and business units to reduce the number of controls that need to be maintained.
Monitoring and Reporting	Business intelligence solutions, and monitoring and reporting software provide automated role-based dashboards with key indicators.

Figure 6: Summary of Capabilities provided by COTS GRC Solutions.

services and XML, can be used to rapidly enable these capabilities across an enterprise.

COTS Risk and Compliance Solutions – A variety of solutions in the marketplace that handle aspects of enterprise risk and compliance, and that provide process control, monitoring, learning, and education and/or performance measurement capabilities.

The use of COTS-based Risk and Compliance applications, in particular, has been a growing trend as organizations seek to streamline their GRC efforts. The capabilities of these software packages range from organizing and documenting an internal control review project, to providing preventative controls that help automate the segregation of duties.

Because of the growing maturity of these products, and the significant benefit that Federal agencies can achieve through their implementation, PwC has developed capabilities around the implementation of these solutions that is a key element of our overall iGRC approach. Three software solutions in particular – Oracle, SAP, and Approva – have been recognized as market leaders based on their ability to deliver end-to-end GRC capability and therefore have been the focus of PwC's solutions development. In general, these vendors provide capabilities in most, if not all, of the areas depicted above in Figure 6:

An agency's decision to select one of these tools to support their GRC initiatives is highly dependent on both their particular environment and specific needs, and also on the individual strengths and weaknesses of the solutions. A general trend, however, is for agencies to utilize GRC applications that integrate well with their back office systems (i.e., use the same vendor for GRC as has been implemented for back office solutions). This is not necessarily a requirement, however, as components of each vendor's GRC suite may integrate well regardless of the back office systems being utilized.

The Right Experience to Address the Governance, Risk and Compliance Challenges Facing Federal Agencies

In-depth Knowledge of Federal Regulations and Requirements

The ability to address the unique governance, risk, and compliance issues facing Federal agencies is significantly enhanced by understanding the laws and regulatory guidance that each organization must address. These regulations, ranging from OMB Circular A-123 that outlines Federal requirements for internal controls over financial reporting, to the Federal Information Security Management Act (FISMA) that measures agencies' compliance with information security standards, require substantial knowledge and insight to properly and effectively implement. This is particularly difficult, as agencies strive to not only comply with regulations but also to implement best-in-class operations and business processes that enhance the mission of the organization.

PwC's focus on the Federal government allows us to quickly shape and channel vital information and advice to clients. It also allows us to share information about challenges facing the Federal sector. PwC has supported over 28 components within 9 agencies on their A-123 (Appendix A) implementations, including the U.S. Fish and Wildlife Service (FWS), the U.S. Department of Agriculture (USDA), the Department of Education, the Federal Bureau of Investigation (FBI), the National Aeronautics and Space Administration (NASA), the Department of Homeland Security (DHS), and the Executive Office of the President (EOP). The experience PwC has gained at these agencies has allowed us to understand in detail the qualities and characteristics necessary to successfully implement organizational business process and technology changes to deliver compliance and enhanced operations. Based on this experience, PwC has been hired by many Government agencies to support the implementation of organizational as well as business process improvemens that help to establish a foundation for sustainable compliance. Figure 7 summarizes PwC's experience relevant to providing GRC support to Federal agencies.

Capability	PwC's Qualifications and Experience
An Independent Public Accounting (IPA) with expertise in internal control and Federal audits	• PwC has the longest tenure of any U.S. IPA performing assessments of internal control over financial reporting in the Federal government sector. • PwC has performed more than 50 Federal audits in the last five years and eight first-ever audits. • PwC has an IT Audit group dedicated solely to performing Federal Government reviews of financial management automatic data processing internal control systems. • PwC was hired by the Government Accountability Office (GAO) to update its Federal Information Systems Control Audit Manual (FISCAM) methodology. • PwC has substantial experience performing internal control assessments with large organizations to comply with both OMB Circular A-123, Appendix A, and the Sarbanes-Oxley Act.
Possesses deep knowledge of relevant legislation, regulations and guidance	• PwC has extensive experience helping Federal agencies implement and comply with the numerous legislative and regulatory requirements that support sound financial management and effective internal control. These rules and regulations include the following: - CFO Act, Federal Managers' Financial Integrity Act (FMFIA), Government Performance Review Act of 1993 (GPRA), Inspector General (IG) Act, Federal Financial Management Improvement Act (FFMIA), Improper Payments Information Act (IPIA), Single Audit Act, Clinger-Cohen Act, OMB Circular A-127 Financial Management Systems, FASAB standards, Yellow Book, Green Book, Federal Information Security Management Act (FISMA) of 2002, and OMB Circular A-130 Management of Federal Information Resources. - GAO's and the President's Council on Integrity and Efficiency's (PCIE's) financial audit methods, as set forth in the GAO/PCIE FAM and the GAO FISCAM.
In-house technical capabilities	PwC is the world's largest professional services organization with a tradition of nearly 100 years of public and commercial services: • More than 29,000 employees in the U.S. • More than 6,500 CPAs in the U.S. • Several former Federal CFOs and senior executives that can be made available for consultation.

Figure 7: PwC's Federal Experience Overview.

Figure 8: Auditor's Perspective.

The Auditor's Lens

PwC understands that the effort of Federal agencies to achieve and maintain an unqualified audit opinion is a significant part of their overall financial management transformation goals. PwC brings an audit perspective to our support for Federal agencies that allows us to recognize root causes of material weaknesses and to discriminate between corrective actions that will, and those that will not, provide sustainable resolution of the conditions. Because we serve as the auditors for several of the largest Federal agencies (e.g., Social Security Administration, General Services Administration), we understand the qualities needed for a robust internal control environment and financial accounting operation. Figure 8 demonstrates PwC's audit perspective to help agencies achieve the goal of an unqualified opinion and the resolution of material weaknesses. Sustainable resolution of material weaknesses is critical to achieving the goals of improved governance over financial resources and operations, and of compliance with Federal laws and regulations.

Experience with iGRC Technology Solutions Most Relevant to Federal Agencies

As mentioned above, PwC has made significant investments in developing solutions around GRC COTS products, and has actually partnered with the software vendors in co-developing their solutions. While we remain independent from these vendors and do not endorse any single product, PwC has developed robust centers of excellence around the Oracle, SAP, and Approva GRC suites. The following paragraphs briefly describe our expertise with these products.

Oracle – Our Oracle GRC capability is comprised of over 500 knowledgeable staff located across the U.S., with deep skills and experience in Oracle applications. The staff includes 50 professionals dedicated solely to Oracle applications GRC projects. Our practitioners, many of whom hold Certified Information System Auditor (CISA) and Certified Public Accountant (CPA) designations, have designed, implemented, and managed GRC solutions in support of Oracle implementations.

Our leadership with Oracle applications has been shown over the years through the development of our cutting edge tools, all of which directly support an Oracle GRC engagement. These tools include the following:

- PwC Global Risk and Control Repository – The PwC Risk and Controls Repository contains comprehensive, best practice business process risks, and related controls tailored for Oracle environments. Our library of risks and controls is organized by business process cycle (e.g. revenue and receivables, purchases and payables, inventory management, financial general ledger), and represents an accumulation of the experience of our ERP risk management practice.
- PwC Business Process Controls Practice Aids – The PwC Business Process Controls Practice Aids are created from our Risk and Controls Repository. These PwC practice aids provide detailed descriptions of each Oracle process cycle, and provide a description of how business process controls should be integrated into each process.
- PwC Oracle Specific Control Tool – Our Oracle applications security and configuration assessment toolkit is developed specifically by PwC for use in the completion of Oracle security and controls projects. This toolkit contains self-extracting SQL scripts that can run against Oracle production databases, the output of which are used to identify over 400 unique application and database configuration settings.

SAP – Our collaboration with SAPGRC provides agencies with their first opportunity to engage a fully integrated, flexible and sustainable governance, risk


U.S. CUSTOMS
and
BORDER PROTECTION
1300
TOW AWAY
NO STANDING OR PARKING
ANYTIME

management, and compliance solution. As a means of helping organizations leverage this technology, we make available the largest global resource pool on the SAPGRC technologies. We are the only firm advising SAP on the GRC vision and strategy that drives the business value of the solution, as well as on how these factors influence the solution's design and capabilities. The GRC-related services we extend to our customers address critical issues both during and after solution implementation. Our solutions help agencies to:

- Define the strategic vision for an integrated GRC program at the most appropriate level – whether enterprise, regional or divisional.
- Conduct a current state assessment of GRC capabilities in comparison with industry-leading practices. Identify gaps and requirements for key risks and controls as well as recommendations for improvements.
- Implement and integrate the solution in accordance with the strategic vision. Address issues such as determining the best approach for migrating manual controls and processes to automated ones and creating dashboards and workflow content that enables reliable, automated processes.
- Customize SAPGRC's solution to specific client needs, preferences and requirements.
- Apply industry-leading practices and content-specific applications to "fast track" implementation.
- Support solution implementation with knowledge and expertise in key GRC-related areas, such as information security, data management, and sourcing.
- Design and configure reporting to meet client regulatory, compliance, and risk management needs.
- Conduct testing, remediation, and training activities to maintain the effectiveness of the GRC program, personnel, and policies.

Approva – Approva applicaitons enable agencies to strengthen their Governance, Risk & Compliance (GRC) programs by extending their continuous controls monitoring and audit processes to new applications and further automating their processes for controls testing, remediation, and sign-offs. Unlike other products, Approva has not specifically aligned with any major ERP Vendor and is built to work with SAP, Oracle, JD Edwards, PeopleSoft, and Hyperion, as well as legacy systems. PwC has a formal alliance with Approva and a practice dedicated to implementing the product. This practice maintains PwC proprietary methodologies and toolsets specific to implementing the Approva GRC applications.

Summary

Federal agencies face ever increasing challenges to comply with a wide array of laws, regulations, and policies impacting their management control environment. Other factors increasing the challenge for Federal managers include the decentralized nature of current compliance efforts and the lack of technology to support the documentation, testing, and reporting of compliance activities. PwC's Integrated Governance Risk and Compliance methodology (iGRC) uses a principles-based framework that can help Federal agencies establish a common set of activities that can be consistently implemented across the enterprise resulting in not only improved compliance, but enhanced businesses processes. This methodology, supported by our in-depth knowledge and experience with Federal agency regulations and our market-leading expertise with GRC technologies, makes PwC the right choice to help Federal agencies meet their compliance challenges.

pwc.com