# Governance and Compliance

All chartered endeavors are required to operate within a set of governance and controls frameworks.  Many are governed by steering committees responsible for the business issues associated with the endeavor that are essential to ensuring the delivery of project outputs and the attainment of program outcomes.  Their scope of responsibility spans approvals of the budget strategy; defining and realizing targeted benefits; monitoring and managing risks, quality and timelines; making policy and resource decisions; and assessing requests for changes to the scope of the endeavor.

Avistas supports these steering committees, executive teams, directors and managers by providing resources, tools and techniques to assure the availability, accuracy and delivery of management information and controls to responsible parties.  The areas below represent some of many management frameworks and regulatory authorities that Avistas supports our clients with related implementation and compliance obligations:

- ► COBIT, Control Objectives for Information and related Technology
- ► Six Sigma
- ► Sarbanes-Oxley
- ► HIPAA, Health Insurance Portability and Accountability Act
- ► GLBA, Gramm-Leach-Bliley Act

COBIT, Control Objectives for Information and related Technology

This framework is essentially used to develop operational maturity and excellence in all areas relating to the union of people, process and technology for business benefit within an enterprise.  It is usually coupled to the Information Technology Infrastructure Library (ITIL), Information Technology Service Management (ITSM), Six Sigma and ISO 17799 (Information Technology – Code of Practice for Information Security Management) practices, to name a few.  While individual client circumstances dictate the choice of frameworks and tools, generally COBIT and ISO 17799 help to define what should be done and ITIL providing the how for service management aspects.

Avistas provides expertise in all of these areas in order to supply discipline and experience to our client's resources when implementing these best practices.

## Six Sigma

This methodology is an intensely data-driven, systematic approach to problem solving, with a focus on customer impact. Within this framework are two key methodologies: Define, Measure, Analyze, Improve and Control (DMAIC) and Define, Measure, Analyze, Define and Verify (DMADV). DMAIC is typically used to improve an existing business process while DMADV is typically used to create new product designs or process designs in such a way that the targeted outcome is more predictable, mature and defect free in performance.

Avistas augments our client talent pool with expertise that can harvest actionable business intelligence from raw data, highlighting vital trends and improving performance while utilizing Six Sigma disciplines.

## Sarbanes-Oxley

Section 404 is the official mandate from the Securities and Exchange Commission on what Sarbanes-Oxley demands regarding financial reporting and controls. It has stirred consternation within many organizations whose executives are averse to wearing stripes due to financial reporting gaps, irregularities and mistakes rooted in process and technology. Chief Financial Officers are most tenacious in enforcing internal audits and controls are often at odds with Chief Information Officers who have traditionally owned and supported the applications and tools used business process and financial reporting.

Avistas professionals serve a vital roles in supporting both of these "camps" in order to implement solutions that move beyond satisfying compliance obligations, but automate and streamline business processes and financial controls so that the cost of compliance goes down over time while business performance improves.

## HIPAA, Health Insurance Portability and Accountability Act

This act of legislation passed in 1996 is a broad reform of the healthcare industry. Within the regulation, the Administration Simplification section has a significant impact on IT and Information Security departments, as well as healthcare software application vendors. Severe civil and criminal penalties threaten healthcare organizations that are found to be noncompliant with HIPAA. IT departments are particularly sensitive to the privacy and security rules. Thus, IT departments are compelled to implement strategies and processes with continuous improvements to:

- ✓ Assure service levels, policy compliance and appropriate risk management
- ✓ Secure all assets and services
- ✓ Control and track all access to protected health information
- ✓ Reduce the cost and complexity of heterogeneous IT infrastructure management
- ✓ Maintain audit trails for all access, changes and distribution of HIPAA protected information

Avistas professionals apply industry best practices to fence these risks and ensure HIPAA compliance while providing further clarity and integrity to operational and performance "Line-of-Sight^SM".

GLBA, Gramm-Leach-Bliley Act

Passed in 1999, this legislative act sinks teeth into corporations' obligations to protect nonpublic personal information.  Section 501(b) specifically addresses, in part the mandate to comply with the Safeguards Rule:

- ✓ to insure the security and confidentiality of customer records and information

- ✓ to protect against any anticipated threats or hazards to the security or integrity of such records

- ✓ to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

For those corporations and businesses under the jurisdiction of GLBA, this requires careful attention to IT organizational, managerial and technical controls including security policies and procedures, risk assessment, incident response, auditing, data integrity, change management, authorizations and approvals to name a few.  Avistas professionals excel at applying proven techniques to ensure compliance with all relevant regulatory and reporting obligations.

## Avistas Practice Areas

### Management
- Business Intelligence
- Project Portfolio Optimization
- Change and Asset Management
- Human Capital
- Acquisition, Mergers and Divestitures
- Governance and Compliance
- Business Process Optimization
- Services Delivery Management

- Knowledge Performance Management
- Program, Project and Product Management

### Technical
- Application Integration
- Infrastructure and Technology
- Development Support

Contact: Bill Morgan
214-544-0400
bmorgan@avistas.com

AVISTAS
The Summit at Las Colinas
545 E John Carpenter Fwy, Suite 300
Irving, Texas  75062
Tel: 214-544-0400
Fax:  214-242-2311
www.avistas.com

**Governance and Compliance**