White Paper

Business Office
11000 SE CR 3280
Kerens, TX 75144

Virginia Office
11921 Freedom Dr,
Suite 538
Reston, VA 20190

Texas Office
500 West Seventh St. Suite 700
Fort Worth, TX 76102

HARMONY TECHNOLOGY SERVICES
A Clear Creek Group Company

Compliance

You can't read the news today without seeing a headline about companies that run afoul of increasingly complex regulations. Let's face it – it's easier than ever to do! Whether a company is publicly traded, involved in the Federal space, or works in any number of highly regulated industries, Compliance is often seen as a minefield of regulations. However, when done correctly, compliance can actually increase profitability regardless of how complex the regulations are within the company's industry.

Introduction

Think back to 25 years ago. Things didn't used to be this complex, or as regulated. Do you remember the time before Gramm-Leach-Bliley, before Sarbanes-Oxley, and before HIPAA? It used to be enough to just "do the right thing." Companies were expected to do the right thing and often did so. It was conceivable that a small department could manage to meet necessary operational and reporting demands.

That all changed following high-profile corporate scandals in the early 2000s (who remembers Enron, Tyco, and WorldCom?). It wasn't long after that, that numerous pieces of legislation were passed, and regulations are written to prevent that kind of free-wheeling wantonness from happening again.

Today, compliance is mandatory. Beyond that though, compliance is almost gravitational, holding the enterprise together. It can be a compass that guides management, providing them with assurances that the enterprise remains on the right path. failure to have robust compliance controls in place can not only lead a company off course, but it can also have enterprise-ending consequences.

In this paper, we will describe the components of strong compliance programs and share thoughts with you about how to take your compliance effort to the next level to create Value and Harmony between the top line and bottom line.

Compliance is doing what you have to… but it's really only one part of strategic risk management.

With the threats that being out of compliance can represent, it can be easy to focus on simply trying to not take a wrong step. That approach, though, is reactive and shortsighted. Smart companies view compliance as one of many components of their overall strategic risk management. In approaching compliance, best practices call for being proactive in taking a holistic, risk-based approach. To a company with a strong compliance program, there are both hard and soft benefits, including:

1. Increasing profitability

2. Driving organizational efficiency

3. Producing a better risk profile

4. Enabling more complete knowledge about the business

5. Achieving recognition in the marketplace

A well-executed compliance program can add value to a company that may potentially be interested in selling or being acquired. It provides more certainty which means less of a discount in company valuation. Conversely, there are significant risks to companies that do not make strong compliance a priority. Negative consequences include:

1. Inefficiency
2. Increased risk exposure
3. Decreased profitability
4. Diminished marketplace value or acquisition advantage
5. Less knowledge of the business
6. Fines
7. Criminal liability
8. Complete business failure

Despite the risks of having a weak or non-existent compliance program, it happens to companies for many possible reasons. Most often, companies are focused on the day-to-day operations. They can simply feel like they are too busy to focus on compliance as a top priority. Still, other companies may be fairly small, or not be structured in a way that enables resources to be applied to compliance. They may also suffer from a lack of resource bandwidth or specific expertise.

Knowing the consequences of noncompliance can help focus a company on the potential risks. Exceptional companies, however, will look past the downside possibilities to develop robust policies to govern the running of the enterprise in not only an ethical way but in a way that also supports the efficient operation. Really, a thorough and rigorous compliance program can yield returns equal to, or greater than, resources put into it.

A system of controls to mitigate risk.

Just as compliance is but one aspect of overall risk management, it takes a variety of controls over many different key parts of the enterprise to minimize the risks that can threaten the enterprise in several ways. It is through the rigorous development and use of controls in the following areas that the enterprise ensures it will run efficiently, be able to meet its contractual obligations, and thrive.

1. Accounting & Financial Controls

Effective financial and accounting controls are critical to accurately and fairly presenting a business' operating results and risk profile. Weaknesses in these controls can contribute to inaccurate or incomplete financial reporting and potentially result in legal fees/fines, significant reputational damage, and a loss of business.

Strong financial controls, on the other hand, support the supervisory interest in maintaining a safe and sound financial operating system. the development of a comprehensive financial control framework is a key component for businesses to maintain an effective control environment and is indicative of a company's culture where management places importance on internal controls.

2. Project Management Institute (PMI)

Since the 1960s, the discipline of project management has become more systematized in the aerospace, construction, and defense industries. In 1969, the Project Management Institute was formed at the Georgia Institute of Technology as a nonprofit organization to "foster recognition of the need for professionalism in project management; coordinate industrial and academic research efforts; develop common terminology and techniques to improve communications; provide an interface between users and suppliers of hardware and software systems; and to provide guidelines for instruction and career development in the field of project management."[3] Today, the organization not only defines standards, frameworks, and benchmarking for project management, program management, and portfolio management. But they conduct rigorous training and credentialing of more than 600,000 practitioners in more than 185 countries, making PMI the world's largest project management member association.[4]

3. Cyber & security controls

Security standards and requirements frameworks are necessary to address and minimize the risks to enterprise systems and the data they contain. One of the most significant challenges companies face is maintaining a forward-leaning defensive posture to do more than reactively address attacks that have already happened. It is critical to have security controls in place that address business processes, system architectures, automation and services, software access, logs monitoring, and patches and download upkeep.

4. Business continuity

Proper controls in this sphere seek to prevent the interruption of mission-critical services to the enterprise. It includes processes and procedures that a business needs to put in place to ensure that essential functions can continue during and after a disaster. A proper plan will address human resources as well as hardware, software, and infrastructure.

5. Data Integrity

Data integrity controls govern how a business maintains and assure the accuracy and consistency of data within the enterprise. Data integrity drives the design, implementation, and usage of those systems that store, process, or retrieve data. In developing controls, one must address both the logical integrity as it pertains to the "correctness" or rationality of any piece of data in its given context, as well as the physical integrity. Managing physical integrity pertains to many aspects related to the physical environment which can include redundant hardware, uninterruptible power supply, system configurations, and file storage systems. Challenges to both logical and physical integrity include design flaws, power outages, equipment failure, electromagnetic faults, and human error.

6. ISO standards

The International Organization of Standards (ISO) is instrumental in ensuring quality, safety, and efficiency in virtually every industry. Their most widely known standard, ISO 9000, arguably has the most impact of all the 13,000 published standards for manufacturing and service industries. This set of standards assesses quality management systems and provides guidance to organizations that want to provide continuous quality improvement while ensuring that their products and services meet their client's requirements.

Another set of standards-ISO 26000-provides guidance on how businesses and organizations can operate in a socially responsible way. Often this can be indicative of a company's overall performance, especially as it pertains to how they contribute to the health and welfare of society at large.

To be ISO certified, an organization must be reviewed by an outside assessor to examine records and interview staff to determine compliance with applicable standards. If certain standards are not met, organizations being assessed will have a specified time in which to correct shortcomings to be certified.

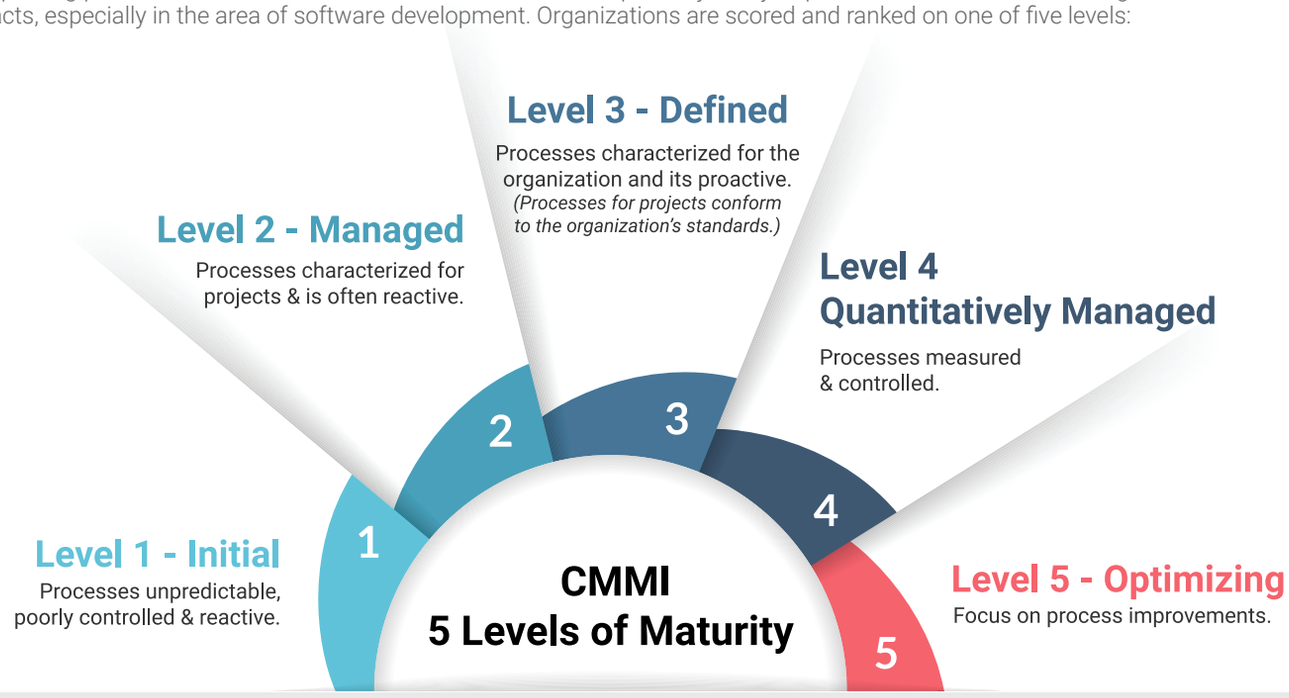
7. IT Service Management (ITSM)

IT Service Management (ITSM) is a discipline that aligns the enterprise with its resources and services to provide an optimal end-user experience. ITSM is built around processes and practices to evaluate the end-to-end delivery of its solutions, measuring operational efficiency to meet service level expectations.

As a subset of ITSM, the Information Technology Infrastructure Library (ITIL) provides a cohesive set of best practices drawn from the public and private sectors. As a standard, it provides consistency in terminology and processes in organizations. As more companies and suppliers develop solutions for their customers, these standards become crucial to ensure that best practices are used to deliver the best solutions. Companies and individuals can become certified in these frameworks to demonstrate increasing levels of competency and qualification.

8. Capability Maturity Model Integration (CMMI)

CMMI is a process improvement training, appraisal program and service developed by a group of experts from industry, government, and the software engineering institute at Carnegie Mellon University. CMMI models provide guidance for developing or improving processes to meet business needs and are often required by many Department of Defense and U.S. government contracts, especially in the area of software development. Organizations are scored and ranked on one of five levels:



The risk/reward calculus

It is the responsibility of both a company's board and senior management to ensure that their company identifies, assesses, prioritizes, manages, and controls risks that could negatively impact the enterprise. A robust compliance program, despite the resources and financial costs it requires, can enhance the value of the company, increase profitability, and improve efficiency. The negative consequences can range from minor to dire.

The calculation that both the company's board and senior management must solve is whether the price of compliance is worth the time, expense, energy, and resources that it takes to execute it. Inevitably, over the long term, the pluses outweigh the minuses. The challenge is having the confidence and long-term vision to put these mission-critical efforts in place.

What drives compliance today?

To understand what drives compliance today, it is worthwhile looking back over the past 90 years to contemplate the historical events and circumstances that led to the creation of key government agencies and organizations that provide substantial oversight of companies and entire industries. Examples of these organizations include the Securities and Exchange Commission (SEC), the Occupational Safety and Health Administration (OSHA), and Health and Human Services (HHS), along with their subordinate agencies – Centers for Medicare & Medicaid Services (CMMS) and the Office of Civil Rights (OCR).

The Securities and Exchange Commission (SEC)

Despite several recent and notable pieces of landmark legislation and regulations, Modern corporate oversight began decades ago. Following the great market crash of 1929, the country saw increasing support for federal regulations of the securities markets that had not existed in the post-World War 1 era and the care-free roaring 20s. After October 1929, with public confidence in the market decimated, congress acted to monitor the securities industry in a highly coordinated way, ultimately creating the Securities and Exchange Commission (SEC) through the Securities Act of 1933 and the Securities Exchange Act of 1934. The SEC's goal "to promote stability in the markets and, most importantly, to protect investors."[1]

The Occupational Safety and Health Administration (OSHA)

Another governmental agency that provides significant oversight into how enterprises in a wide variety of industries conduct their business is the Occupational Safety and Health Administration (OSHA), created by Congress through the Occupational Safety and Health Act of 1970. As a part of the Department of Labor, the agency acts "to assure safe and healthful working conditions for working men and women by setting and enforcing standards by providing training, outreach, education, and assistance."[2] Health and Human Services (HHS) became responsible for the adoption of national standards for electronic health care transactions and code sets, unique health identifiers, and security following the passage of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). After that legislation was passed, HHS published a final privacy rule and security rule providing additional clarity and guidance in the form of administrative simplification provisions, some of which are administered and enforced under the HHS umbrella by the Centers for Medicare & Medicaid Services (CMMS), and others by the Office for Civil Rights (OCR). To ensure that technological advances didn't erode information privacy, responsibility was given to OCR to investigate complaints and conduct compliance reviews to determine if covered entities are in compliance with the requirements of the privacy and security rules. While there are certainly other governmental agencies that have authority over how many of the businesses in this country operate, these three touches many in profound ways. Key pieces of legislation and new regulations enacted and implemented over the past ten to twenty years have also reshaped the business environment.

The Dodd-Frank Wall Street Reform & Consumer Protection Act

In addition to existing federal regulations, financial service organizations face new regulatory challenges in the Dodd-Frank Act – but that's not all. There are also unique regulations in each of the 50 states. Despite operating in an increasingly complex regulatory environment, many financial services organizations today approach regulatory compliance in a reactive mode after bad things happen. The risks of not being more proactive include penalties, fines, litigation, and potentially negative media coverage. The Sarbanes-Oxley Act of 2002, sponsored by Paul Sarbanes and Michael Oxley, represented a significant change in federal securities law. Also known as SOX, SARBOX, or S-O, it required all publicly traded companies to implement and report internal accounting controls to the SEC for compliance. Effective in 2006, the act includes criminal and civil penalties for noncompliance, certification of internal auditing, and increased financial disclosure. It affects public U.S. companies and non-U.S. companies within the U.S. Presence. The Sarbanes-Oxley Act requires all financial reports to include an internal controls report. This shows that a company's financial data are accurate, and adequate controls are in place to safeguard financial data. Year-End financial disclosure reports are also a requirement. A SOX auditor is required to review controls, policies, and procedures during a section 404 audit. SOX auditing requires that internal controls and procedures can be audited using a control framework like COBIT. Log collection and monitoring systems must provide an audit trail of all access and activity to sensitive business information. From a system perspective SOX sections 302, 404, and 409 require the following parameters and conditions to be monitored, logged, and audited:

- **Internal controls**
- **Network activity**
- **Database activity**
- **Login activity (success & failures)**
- **Account activity**
- **User Activity**
- **Information access**

Besides lawsuits and negative publicity, a corporate officer who does not comply or submits an inaccurate certification is subject to a fine of up to $1 million and ten years in prison, even if done mistakenly. If a wrong certification was submitted purposely, the fine can be up to $5 million and twenty years in prison.

Taking your compliance to the next level

To have a truly robust compliance program, a company must undertake a structured approach to ensure a thorough job is done. You must have the proper tools and processes in place to demonstrate that your organization has an effective compliance program in place. Ideally, you will wind up with a system that will:

- Streamline your compliance process across the enterprise.
- Provide global visibility to compliance-related matters across the enterprise.
- Act as the "compliance system of record", supporting a state of continual readiness for audits.

To structure a strong compliance program, companies are smart to follow certain prescribed steps to ensure success. These steps include:

STEP 1. Inventory of policies & procedure

When done for the first time, use the results as a baseline measurement. Evaluate the results to determine areas of opportunity where improvements can be made.

STEP 2. Identify the applicable frameworks that will cover compliance in your organization

The industry you are in and the legislative and regulatory confines in which you must operate will define much of this for you. This may differ based on whether you are a publicly traded company, deal with the federal government, or work in the healthcare space.

STEP 3. Identify gaps between formal control frameworks and systems

Once you have defined the frameworks under which you will operate and have inventoried your current policies and procedures, it becomes crucial to identify where gaps exist. Once done, a company must work to tighten up controls, policies, and procedures to eliminate them.

STEP 4. Establish automated controls

Where possible, it is almost always in the best interests of the enterprise to automate systems in compliance-related matters. Typically, you will see this around accounting functions, inventory control, financial reporting, corporate training, and human resource functions.

STEP 5. Enact Standards

This may apply to the federal acquisition, cost account, or Government Risk & Compliance (GRC) tools in the ERP. The goal is to dictate what standards will be followed within the company and then stick to them.

STEP 6. Command media/process documentation develop & review

It all comes down to making sure that you are doing what you have identified as necessary and prudent. It is not, however, just a one-time event. It requires periodic review, and when it is done well, it can lead to improvements in process optimization.

How to create value and Harmony between the top line and bottom line

An effective compliance program is a value that's added to the top-line investments to result in better bottom-line outcomes. Compliance starts with best practices. The Harmony Technology Services approach is a cycle of people, processes, and technology, with each part influencing the other two. We can jump in to analyze this at any point, but let's begin with the process, which refers to determining. Whether a company is operating in a way that is consistent with best practices or if some adjustments are needed. The tools the company employs to complete these processes make up the technology component, which focuses on making sure that a system is acting the way it's expected to. From that point, in the people component, you determine what technologies and processes people are having issues with and focus on resolutions there.

Describing Success

Generally, the most successful companies are those that believe that when they find a problem, they need to fix it. In the case of compliance, it requires acting before a problem exists. So, how does one know that implementing a rigorous program was successful?

Here are some of the measures that can help you identify success:

- Revenue, time to market, and quality all increased because of better policies.
- Automated systems have been fully leveraged and optimized.
- The way the company measures and reports business results has matured.
- Automated workflows have been implemented to have better controls, audit paths, and reporting, working faster and more accurately.
- Measures of compliance have been built into processes.
- Fewer people are doing the same job (i.e., better procurement with more controls that take fewer staff)
- The number of audit findings and corrective actions has decreased.

As it relates to cyber security:

- The time that vulnerabilities exist have been minimized.
- Vulnerability over time from an established baseline has decreased.
- The patching lag time from release to deployment has been reduced.

Conclusion

The Harmony Technology Advantage

It used to be that the company relied on only one or two software packages to run their business, and controls were more people/process driven. Now, however, successful management of compliance-related matters often comes down to successfully managing both processes and technology. Often, it's about bringing process optimization and compliance together and enabling them with robust systems.

Harmony Technology Services have extensive expertise in industry verticals that are heavily dependent on software controls. Harmony Technology Services also shines a light on inefficiencies in a company's processes that often go overlooked. With extensive experience in Sarbanes-Oxley compliance, our principals bring Fortune 100 C-level experience to those challenges, after having led both internal operations and outsourcing programs in the private and public sectors.

Agile, flexible, and responsive, Harmony Technology Services represents the coming together of practical experience, technological vision, financial acumen, and personal accountability – especially when it comes to challenges related to compliance. Our teams of engineers and project managers bring creative, cutting-edge problem-solving… and a world of experience… to your business challenges. We team effectively at all levels of your organization – from the executive suite to business process owners and subject matter experts.

THAT'S THE POWER OF HARMONY.

For more information about how your company can be effective and reduce the risk of being out of compliance, contact Harmony Technology Services via email at **info@harmonytechnologyservices.com**

RESOURCES

Harmony Technology is dedicated to Improving Value-based Care & Provider Network Optimization

References

End Notes:

1. source: http://www.sec.gov/about/whatwedo.shtml#create
2. source: https://www.osha.gov/about.html
3. sophie j. Chumas & joan e. Hartman (1975) directory of united states standardization activities nbs special publication 417. P. 141
4. source: http://www.pmi.org/~/media/pdf/certifications/pmi-certifications-brochure-2014.ashx

Contacts

Josh Shelman

Director of Business Development

josh.shelman@harmonytechnologyservices.com

817-879-3787

www.linkedin.com/in/josh-shelman-b79039a

James Staggs

IT Program Director

james.staggs@harmonytechnologyservices.com

682-319-4624

www.linkedin.com/in/jstaggs

Contact Us

Business Office
11000 SE CR 3280
Kerens, TX 75144

Virginia Office
11921 Freedom Dr,
Suite 538
Reston, VA 20190

Texas Office
500 West Seventh St. Suite 700
Fort Worth, TX 76102

www.harmonytechnologyservices.com

info@harmonytechnologyservices.com

817-227-2104