Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

The Maturation of Controls Self - Assessments

This topic is appropriate for the Global Security Leadership Certification because it provides IT leaders with practical information and historical references. This paper provides the history of why compliance and controls are a necessary part of society and business. It will also provide the origins of the control self-assessment process and the detail needed to create, manage and mature a control self-assessment program. It also addresses how to demonstrate to senior management their ability to add value, reduce expe...

Copyright SANS Institute
Author Retains Full Rights

AD

The Evolution of Controls and Compliance

GIAC (GSLC) Gold Certification

Author: Timothy Salka, TSalka01@gmail.com
Advisor: Kees Leune

Accepted: July 30, 2014

Abstract

This topic is appropriate for the Global Security Leadership Certification because it provides IT leaders with practical information and historical references. This paper provides the history of why compliance and controls are a necessary part of society and business. It will also provide the origins of the *control self-assessment* process and the detail needed to create, manage and mature a control self-assessment program. It also addresses how to demonstrate to senior management their ability to add value, reduce expenses, maintain innovation, and improve customer acceptance, while increasing the overall security posture of an organization. Additionally, I demonstrate a direct correlation between strong business performance and the existence of a well-managed controls program. Gulf Canada determined that their best performing businesses had management teams that embraced the integration of local controls into their business processes. These controls directly impacted the productivity, quality and profitability of that business

If accountability, transparency and ownership do not lie in the hands of those assessing themselves, the program will fail to be successful. Governance is the key role of the Information Security Department in making the controls self-assessment program a success.

© 2014 The SANS Institute Author retains full rights.

1. Introduction

From a philosophical and historical perspective, I have come to believe that, at its core, the act of compliance is rooted within historical law. Dating back as far as 1772 BC, history shows us examples of the evolution of regulation and the harsh consequences that some have paid for lack of compliance to law.

There are many examples of abuse and corruption in some of the first English based corporations established as early as the early 1700s (Dragomir, 2009). Although America gained its freedom from Great Britain on July 4, 1776, it did not show greater reverence toward holding itself to higher standards of financial reform during in its formation. From the great depression of the "1920s", through Enron scandal and the housing bubble of the 21st century, there continues to be new scandalous events that contribute to the further emergence and maturation of controls in American. It was only through crisis or harsh punishments that early formations of business and individual behaviors were shaped (Hermann & Johns, 2004). In early public law the cost of putting out another person's eye or injuring another's limb would simply be rectified by putting out the eye of the accused or breaking their limb as a means of legal retribution. In today's society a more powerful approach was introduced in 2002, the Sarbanes Oxley Bill (Peavler, 2014). This law holds corporate executives criminally and civilly accountable for the inaccuracy of financial reporting.

Laws and Codes have many applications in our society. In simple terms, they are written words that are designed to protect the overall safety of all people within a community. The act of enforcing laws is the process of making sure that there are several levels of accountability, transparency and ultimately compliance to the written words. The formalization of law addresses issues in writing, but the value people put on adherence to the law is what shapes behavior and strengthens enforcement.

From a business perspective, controls can be perceived as red tape and corporate bureaucracy but the facts show that Gulf Canada's management teams that embraced the integration of local controls into their business processes had increase productivity, quality and profitability of that business (McCuaig, 2014).

© 2014 The SANS Institute Author retains full rights.

2. History of Compliance in the 17th century

2.1 Compliance rooted within law

The principle of Law dates a far back as the 1772 BC to King Hammurabi the 6th King of Babylon. Babylon is documented as being the leader of the world's first major metropolitan area. The reigning King, Hammurabi, was known as a great leader of his time. The most notable contribution of his rein was the laws or codes he documented and enforced, known as the Code of Hammurabi. These codes at the time were the basis for law and established a clear punishment or reciprocity system for all the citizens including the likes of slaves, free men and even magistrates such as judges and officials (Hermann & Johns, 2004).

These codes were inscribed on a large eight foot tall stone in the center of Babylon. It was publicly displayed for all citizens to read and obey. It was clear that reading, understanding and abiding by the code was of utmost importance. Lack of compliance with the code would result in physical or monetary punishment. The codes were simple, yet effective; some of the original codes are still referenced today; not as law, but as metaphors from the past. The Hammurabi code is the origin of common phrases still used today, such as an eye for an eye, and a tooth for a tooth (Hermann & Johns, 2004). Primitive and barbaric in comparison to modern day law of the 21st century, but also the origin of rules and the foundation of law from which modern day society developed

2.2 Compliance within religion

Organized groups with shared beliefs contribute to the growth of law. Christians have the Ten Commandments and other biblical teaching such as the Old and New Testament that they follow (Durand, 1912), while Muslims have the Moral teachings of Islam (Badawi, 2010) which follow a shared lawful and unlawful Islamic moral code.

2.3 Compliance within emerging commerce

© 2014 The SANS Institute Author retains full rights.

I have noted laws that guide in the ruling of societies of nations and those that are reflected in religions, but there is so much more to evidence the emergence of compliance. There are other historical dealings, such as the establishment of chartered corporations in England that demonstrated the need to eradicate the existence of impropriety and corruption of corporations through the introduction of law.

According to Corporations have a long history in the English speaking world. They emerged in medieval times as a means by which a group of private citizens could combine their interests under a royal charter to differentiate (and protect) themselves from the changeable interests of the government. Early examples of chartered corporations include the East India Company, formed in 1600 to hold a monopoly on trade with India, and the Virginia Company, formed in 1606 to develop the land and trade opportunities in North America. Valuable monopoly provisions were included in a charter granted to the original founders of the Bank of England in 1694, which was quickly capitalized by public subscription of shares in the London market (Dragonmir, 2014).

2.4 The Sword Bank and Insider trading

In 1710 the Sword Blade Bank of England was involved with insider trading to boost corporate profits by buying larger amounts of unsecured government debt before publicly announcing that the entity and the British government agreed it would exchange its shares publicly. The results of this insider trading would drive up the value of the earlier debt purchases and make the executives of the company huge profits. (Narron & Skeie, 2013; Corruthers, 1996; Dale, 2004)

2.5 The South Sea Stock Valuation Bubble

The History of corruption has a way of repeating itself. In 1711, the South Sea Company was a government supported monopoly created with the intent to exploit export opportunities in South America. The company was formed during the War of Spanish Succession and had little chance of actually achieving its intended financial objectives because France and Spain were strong allies in the region and had a stronghold on the market. This did not stop the major shareholders and officials of the South Sea Company from promoting the sale of company stocks

© 2014 The SANS Institute Author retains full rights.

to eager buyers looking to get a piece of the new market. The company was falsely inflating the valuation of the company to draw investors and its officials had ties to the corrupt leaders whose origin was from the Sword Blade Bank. The South Sea company was bribing the government to buy its national debt which would lead to huge profits for just a few business elites. This trading was also one of the first cases of exchanging government debt for company shares. The promise of huge profits for investors of the shares was nothing more than a façade to get them to buy the overvalued stocks. The stock's value was continually over inflated which eventually led to the its collapse and massive financial losses for those holding the stock. It was documented that due to the South Sea Bubble the loss of confidence and loss of investor trust took over one hundred years before the next publicly traded company was established in England. (Narron & Skeie, 2013; Dale, 2004)

2.6 Adam Smith and the Wealth of Nations

The Scottish Philosopher Adam Smith, an emerging economist and theorist, wrote one of the first books on the impact of political influence on the economy. (Butler, 2007; Eamonn, 2007; West, 1976) Adam Smith was highly connected to in influential people of this era. He was quite scholarly and widely recognized as having associations with the likes of Benjamin Franklin, one of the founding fathers of America. He became famous for his book, The Wealth of Nations which was published in 1776, and is considered to be a significant proponent in the formation of the field of economics and its development into an autonomous systematic discipline in the Western world. Smith proposed that a people's economic status be measured by the volume of production and business not by the volume of gold kept in its treasury. (Butler, 2007; Eamonn, 2007; West, 1976) Some say his principals help form what we call today to measure a countries success as Gross Domestic Product (GDP).

Smith's scrutinized the English government's questionable bailouts. He exposed the misuse of taxpayer's money in the bailout of the East India Company. Through his lectures and works he may have also indirectly influence American history through Benjamin Franklin. Please note that this is not a fact but a theory which I derived from my research. (Butler, 2007; Eamonn, 2007; West, 1976)

© 2014 The SANS Institute Author retains full rights.

3. American Independence

British colonists settling in the America felt they had little representation in this new land. They had little say in what laws, taxes and religions England would bestow upon them. American settlers were exposed to the same corruption, self-serving government controls and excessive taxation as the taxpayers residing in England (Heritage Foundation, 2014).

Ironically, organized colonies evolved and with them came leaders of the new world. Benjamin Franklin was one of those leaders. He worked with Thomas Jefferson, the third President of the United States and one of the principal authors of the Declaration of Independence. The Declaration of Independence was documented in 1776, the same year the Wealth of Nations was published by Adam Smith. Some believe that Benjamin Franklin's professional relationship with Adam Smith had an impact on his political beliefs and aspirations (Smith, 2014). Ben Franklin also participated in the creation of the US Constitution, the framework of the newly formed United States government. Franklin was a professional printer and journalist; his experience in these fields helped him in documenting the code and values within these historical documents. The significance of documentation cannot be undervalued as they left established a future constitution to measure compliance against.

3.1 Emerging Corporate Governance in America

The economic growth of the Unites States following the end of World War I was quite extraordinary. There was a high use of consumer credit to fund these so called Roaring Twenties (Scott, 2006). There was also a lack of consumer saving; it appeared most everyone during this time had a lot of fun, dressing in extravagant suites and stylish dresses, riding in fine cars and buying all the latest technology for the time, like televisions and radios. Eventually consumer buying sprees and the days of lavish living could not be sustained; corporate credit dried out for consumers and businesses and the economy collapsed. It was nine good years of economic growth that ended in the worst financial crisis in America, the Stock Market Crash of 1929.

The economic boom of the 1920's ended with the stock market crash of 1929 and a decade of depressed economic times. The resulting securities acts of 1933 and 1934 brought the first sweeping legislative attempts to regulate the securities market and bring reform to

© 2014 The SANS Institute Author retains full rights.

corporations in the US. With reform comes rules and with rules come compliance to them. Little by little, crisis by crisis, people started to understand the need for reform (Scott, 2014).

When generations of people go through decades of poor economic times, there are some positives. Some people that lived through that time developed greater values, harder wok ethics and determination. A large dose of humility can change behavior of a nation's people. When people have a greater appreciation for values they are more apt to embrace those things that can provide them with a framework from which to limit risk such as controls.

3.2 First Documented Control Self-Assessment Process

In an effort to mature adherence the rules, laws and policies, Gulf Canada became the first known entity to formally create self-monitoring frameworks for adherence to controls known as a Controls Self-Assessment. The Institute of Internal auditor's definition of a controls-Self Assessment is as follows. A Control self-assessment (CSA) is a technique that allows managers and work teams directly involved in business units, functions or processes to participate in assessing the organization's risk management and control processes. In its various formats, CSA can cover objectives, risks, controls and processes. Internal auditors can utilize CSA programs for gathering relevant information about risks and controls; for focusing audit work on high risk, unusual areas; and to forge greater collaboration with operating managers and work teams. Managers can utilize CSA programs to clarify business objectives and to identify and deal with the risks to achieving those objectives (McCuaig, 2014).

A Controls Self-Assessment is nothing more than a self-test of specific controls of a specific job function to ensure adherence to a set of controls. The test is done with some oversight to ensure the process is clearly understood. The participants are normally those involved with the direct operational oversight of day to day operations with key functional and operational managers that enforce their departmental controls through the year. The group is asked to perform these self-check of processes and procedures with their departments. Some may call this the fox watching the hen house but other views this as a means of checks and balances in an effort to stay on track.

Most large corporations are made up of many locations and entities. When compliance issues are categorized, combined and analyzed after collected, you will find that some risks

© 2014 The SANS Institute Author retains full rights.

across its businesses repeat themselves. This is the type of information is valuable because you can use this data to drive change which could have a significant impact across your enterprise.

3.3 Gulf Canada and the emergence of a control self-assessment

One of the founders of the first controlled self-assessment was Bruce McCuaig. I interviewed Bruce on April 23, 2014 about his experience with developing the first ever controls self-assessment while working at Gulf Canada. I preface my documentation in this section of my paper by noting the oil business and the processes described by Mr. McCuaig are much larger and more complex that what I have described. I did this in an effort to keep the paper focused on a high level view of the emergence of a control self-assessment process at Gulf Canada (McCuaig, 2014).

Mr. McCuaig started his audit career at Ernst and Young and was soon appointed Chief auditor at Gulf Canada in the early 1980's. During his tenure he managed approximately 90 staff auditors that would audit business segments such as oil refineries, terminals, service stations and joint venture agreements and others of Gulf Canada.

Mr. McCuaig understood there was a growing concern, originating from many Gulf Canada controllers, who felt they were not getting enough transparency from the Gulf businesses during the normal audit process. There was also a major incident which exposed managers of Gulf Canada of conducting fraudulent activities in the propane sector of their business. Some managers had gotten involved in a number of self-dealings by forming private companies that was supported by Gulf Canada business purchases**.** The accounting centers also identified a few gaps that existed in the ability accurately audit inventory. Mr. McCuaig was engaged by senior leadership to see if he could solve some of these problems. Mr. McCuaig and his General Auditor Paul Makosz established a process by which they would interview the different business sectors such as refineries, terminal service centers, joint ventures and stations. The goal was to determine what the top ten concerns were of the managers running these site level operations. The interviewing process was also used to gather intelligence from the best performers of the different business segments. It was ascertained that some businesses could not adequately run a business if they could not define the significant of the controls that they had in place. Businesses with weak business controls, or, in many cases, the lack of controls, reflected the poorest

© 2014 The SANS Institute Author retains full rights.

performing businesses of Gulf Canada. Typically, businesses that were neither cooperative nor transparent in revealing their processes were the worst overall performing businesses of Gulf.

Those businesses that demonstrated the behavior of being forthcoming and transparent around how they ran their business were some of the most successful sites of Gulf Canada. The best performing locations were willing to share their processes because they ran their business well and they were proud of them. These sites had the best processes and controls in place and ranked highest in their assessment process and as well as running their business. This direct correlation between strong controls and the best performing business led to Gulf's realization if the controls of the best performers were implemented at the poorest performing sites there was lot of upside opportunity at increasing those businesses production capabilities (McCuaig, 2014).

3.3.1 Gulf Canada an internal controls strategically

The valuable information obtained from the numerous Gulf control evaluations went into the creation of a benchmark of controls taken from the top performing business sectors. Mr. McCuaig and Mr. Makosz decided to adopted R. J. Anderson's external audit process as the framework that they would use to present their assessment strategy to the Gulf Canada audit committee. In order to evaluate like characteristics, Mr. McCuaig and Mr. Makosz collected all the control information from their field work and audits. They grouped all the information into seven groups. Controls were categorized into these seven key areas. With this implementation of standard benchmarks for all the different businesses, Gulf management had a way to measure each of their businesses sectors against a control standard or benchmark. This resulted in the ability to chart the results and create metrics for senior management (McCuaig, 2014).

The first area of review was Organizational Controls; these controls focused around on how Gulf Canada managed to react in a timely fashion to organizational changes, such as a plant closure or leadership change, which could have an impact on both upstream and downstream business segments. System Development was the next group where they evaluated their businesses controls. Back in the early 1980's, Gulf Canada, like most other businesses in the decade, viewed system development controls as a service and overhead, as opposed to wealth of useful information. It was a means of getting financial information, but it had little strategic application. The third group was Reporting and Accounting; this was a challenging area for Gulf

© 2014 The SANS Institute Author retains full rights.

Canada to get their arms around. The problem was that they had to rely on the reporting and controls from refineries, terminal service centers, and joint drilling ventures, which was very difficult to control. At the corporate offices Gulf had strong authorization and reporting controls, but in the field the accounting controls could not be heavily relied upon to certify the accuracy of revenues and cost reporting. This was an area of Gulf's controls program that they identified as a significant issue that they needed to improve on. Safeguarding was the next area; this is referred to today as Business Continuity Planning. This was also a challenge as much of the plan relied on functions of the business that were separate, unique and not always available. The next area reviewed was Management Supervisory. This section was in good shape as most of Gulf Canada's corporate offices were well staffed with talented professionals willing to help all the business sectors to establish their goals and objectives. The last section, Documentation control, was not kept up well by the lower performing business sectors. This was more a matter of discipline and the lack of belief in the value of system development and change control for systems. Historically this was a behavioral issue, but to be successful it had to be engrained in processes and have management's full backing.

3.3.2 Let's teach the business

One of the fundamental issues was the inability to accurately measure crude oil production. How much water versus oil was being pumped from the ground was a challenging and critical issue in their business that they needed to learn how to better control.

Mr. McCuaig and his team would visit field office sites frequently. They were determined to ensure each of the businesses would adopt the control standards and associated activities required to meet the business production efficiency objectives. They had large training sessions from all levels of the organization to drive home the compliance messages from corporate. Benchmarks were beginning to be engrained at each business so corporate could now measure businesses adherence to specific controls.

Mr. McCuaig key team members Mr. Makosz and Mr. Leach continued to build the program at Gulf Canada. They would provide the Board with a comprehensive binder to report the quality of the self-assessments at each site. They added a scoring framework made up of five rating levels. This was used to better measure the maturity of each businesses against compliance

© 2014 The SANS Institute Author retains full rights.

objectives from their seven control groups. This rating scale showed the maturity of the control against the desired state. A bar graph for each of the seven control groups was used to show the current status and improvements from prior years (McCuaig, 2014).

3.3.3 Self-Assessment Integration and quality

Gulf soon required self- assessment from every sector of it core business segments, such as oil refineries, terminals, service stations and joint venture agreements. Controls would be the baseline for operational excellence and managers were required to run their business in alignment with the Gulf Canada's controls framework. Workshops and anonymous voting was established to review and evaluate the implementation of new or changed controls. This became an effective way to get full support on changes and align the strategies amongst company leaders.

Gulf understanding of their controls could now could be tied them into meeting business objectives so control weaknesses could now influence their corporate expenditures and budgets. Gulf deployed integrated financial systems, seismic oil measurement and detection systems for their refineries and other business. This showed positive result in Gulf's the ability to accurately measure oil production at their refineries. When the correct operational, financial and security controls are in place, business profitability is positively impacted; however, controls alone are not enough, the need to continually shape human behaviors goes hand in hand with control acceptance and execution (McCuaig, 2014).

4. The Enron Scandal

In 2002, there were more than a few scandals in the United States. But at the top of the list was the Enron debacle. (Peavler, 2014) Enron was an energy broker based out of Houston, Texas. This was a new type of American business that emerged as a result of the deregulation of the oil and gas business. Enron looked to capitalize on the cost of energy by amassing large interests and ownership in this industry. By controlling the sources of energy sources, it could sell the availability of it for huge profits, creating somewhat of a controlled monopoly of services in specific regions of the country. This was most obvious when an electrical blackout occurred in California and Enron made billions by controlling the available energy supply. Even though

© 2014 The SANS Institute Author retains full rights.

billions were made, billions were also lost. (Peavler, 2014) Enron was huge risk taker and when things went bad they were running amuck to hide secrets of corruption. Enron made shady dealings by subvertly controlling energy operations internally and externally. Senior Enron leaders Enron also intentionally falsified earning to increase its stock price. This corruption allowed senior management to embezzle shareholders and employees money. In the end Enron stock was worthless and all those that had invested through the stock exchange or through the Enron investment account lost all their money. The American public was victims of corporate corruption, so in response senator Paul Sarbanes and Representative Michael Oxley crafted The Sarbanes Oxley Act. This legislation was introduced to reform corporate governance and financial reporting. This act was put into law in July of 2002. (Peavler, 2014)

4.1 Regulation of Corporate Governance

With the new reform standards for public accounting firms, corporate management, and corporate boards of directors, the Sarbanes Oxley Act became the most historic government reform of the 21st century.

The Sarbanes Oxley Act addressed many of the reporting issues behind recent corporate corruption and accounting failures. In an effort to focus on the sheer magnitude of lack of compliance with the act, I will highlight the consequences of not complying with the act as noted in sections 302, 304, 802, 906, and 1102. These penalties are expected to discourage corporate accounting fraud by holding CEO's and CFO's personally accountable (Kleckner & Jackson, 2004).

4.1.1 Sections 302 and 906

These pieces of the Sarbanes Oxley Act require corporate CEO's and CFO's to quarterly affirm and certify financial reports filed with the Securities and Exchange Commission (SEC). Deliberate violation of the certification process is subject to criminal consequences with penalties of up to $5 million and up to 20 years in jail (Kleckner & Jackson, 2004).

4.1.2 Section 304

This section also penalizes senior executives monetarily. If their corporation must change its financial statements due to significant noncompliance, wrong doing, or incorrect financial

© 2014 The SANS Institute Author retains full rights.

reporting the CEO and CFO must reimburse any bonuses, incentive-based compensation and profits resulting from the sale of its securities received during the 12-month period following announcement of corporate financial statements (Kleckner & Jackson, 2004).

4.1.3 Sections 802 and 1102

Enron was not the sole culprit accountable for the fleecing of its shareholders and employees. Its accounting firm, the now defunct Arthur Anderson, turned a blind eye when auditing Enron's unlawful accounting practices. They also intentionally shredded tens of thousands of Enron-related papers when they knew they were going to be investigated, so the act also created and enforces penalties and fines to punish those who disrupt an official legal investigation (Peavler, 2014).

Section 802 has two provisions that address the destruction of corporate documents. The first addresses documents within a company: Section 82 states, "Whoever knowingly alters, destroys, mutilates, conceals, or falsifies records, documents or tangible objects with the intent to obstruct, impede or influence a legal investigation, shall be subject to fines and or up to 20 years of imprisonment" (Kleckner & Jackson, 2004).

The second provision addresses a company's auditors, Section 1102 states, "Auditors must retain records relevant to the audits and reviews of financial statements filed with the SEC, including work papers and other documents that form the basis of the audit or review, as well as correspondence for a period of no less than seven years".

5. Control Frameworks

With the new and powerful United States legislation in place senior executives were motivated to ensure that their corporations were compliant and that there executives were safeguarded. The Internal Audit department of American companies had the leading responsibility for most organizations to get their teams and processes in alignment. There was an unprecedented new demand for audit personnel; this is how many people, including myself, transitioned from an operations based role to the role of an IT Auditor. If you had good IT skills and good interpersonal skills, you were heavily recruited to fill the gaps left by the shortage of formal accounting firm auditors. The Vice President of Internal Audit at Textron at the time was

© 2014 The SANS Institute Author retains full rights.

Mike Gardner. Mike was a great leader and was well respected, so when Mike approached me, I was more than willing to take the plunge and learn how to be an IT auditor. The original Committee of Sponsoring Organizations COSO and Control Objectives for Information and Related Technology COBIT frameworks were the backbone doctrine for mapping out financial and IT structures into strategic processes and controls. Most companies referenced COSO, (The Committee of Sponsoring Organizations) which is the embodiment a shared vision of five private organizations dedicated to providing thought leadership through the improvement of in enterprise risk management, internal control and fraud deterrence and COBIT (Control Objectives for Information and related Technology) as their original authoritative source for the SOX governance model.

Regardless of what controls framework is used, the main purpose of a controls program is the enforcement of policies and standards in order to be in compliance to the authoritative source that has imposed governance over your organization reporting and operational requirements.

In my opinion, there are a number of tools to achieve this, but the best method to addresses compliance oversight is a strong controls self-assessment program. A solid controls self- assessment program can cover broad as well as specific controls. It can complement a plethora of other information security initiatives and such as security awareness monitoring a and best practices

5.1 Controls Self- Assessment

I have spent a good part of the last ten years developing and overseeing the Control Self-Assessment process for large enterprise corporations with global footprints. In this paper, I share my knowledge and field work experiences in an effort to assist my fellow Information Security and Compliance professionals. In brief, an organizations control self-assessment tool is the embodiment of a formal governance process which has arisen do mostly impart to seeking standardized and effective enterprise risk and compliance objectives. The results of a Control Self-Assessment (CSA) can provide strategic direction, oversight, and monitoring of corporations controls both at headquarters and at a site level. Controls can be created to meet the requirement of a governing body, state, local or federal law or just compliance to an organizations Information Security program.

© 2014 The SANS Institute Author retains full rights.

Organizations may differ on this point, but generally controls self-assessment is not an audit. Instead, it is a self-check, like going to the doctor for your annual checkup. It is an effective tool to identify changes in security and operational procedures resulting from employee turnover and loss of tribal knowledge. It is the constant reinforcer that only changes when the key stakeholders agree to changes. A control self-assessment is equivalent to having the answers to a test before you take the exam. All you need to do is ensure that the correct answers are reflected in the established practices which the objectives. A control self-assessment is generally free of scrutiny from company boards and calming assurances should be provided to the participants to get good cooperation and useful information.

5.2 Content of Control Self- Assessment

The content of a controls self-assessment is generally developed from a control framework that typically covers numerous security domains. It is also created to satisfy the requirements of authoritative sources which can govern specific functions of either public or private companies. Publicly traded and companies with certification or such as International Organization for Standardization ISO or Payment Card Industry PCI require regular testing as part of monitoring to identify if the control activities are functioning as management has intended. Demonstrating adherence to your controls program also is important for maintaining and renewing certifications. Whether you're using canned controls questions available through the authoritative source or questions that you have developed to align your organization with your Information Security Management System, the information should be kept and maintained in the form of a question library.

Your question set should be able to serve both targeted control self-assessment and general control self-assessments. A targeted assessment may focus on a specific information security domain like physical and environmental for a data center review. There are also authoritative sources that require certain controls be added to the controls self-assessment questionnaire.

Technology changes rapidly, so question sets should be changed to accurately and correctly validate the requirement of your authoritative source. On an annual basis you should evaluate the control self- assessments question set to determine if it is still accurate, or needs

© 2014 The SANS Institute Author retains full rights.

some word smiting based on how easily or not the question was understood by the assessments targeted audience and other participants . If a simple questionnaire does not exist for your targeted subject you can start building a simple baseline of security questions. The SANS list of 20 critical security controls (SANS, 2014) is a good reference to determine if there are any control gaps in your baseline that you might want to add to your program. Also look to address the obvious and high vulnerabilities and common security incidents by adding control activity questions that mitigate them because many incidents come from obvious control gaps. Depending on the size or function of your organization the number of questions can very but, I generally like to see the number of questions in the control self-assessment to be fifty to seventy five, beyond that it takes multiple meeting to complete and you end up with more data than you can use before it is obsolete. Keeping the questions to a manageable level allows you to accomplish more with less information. To create your own questions, take all the relative controls from the environment that is in scope and reframe the control activity in the form of questions. It is the activity that enforces the control that the question should be created to measure.

5.3 Accountability

Accountability is frequently poorly defined and not always upheld. It is important to get senior management support to support enforcement of the process. They should clearly communicate this message to the main stakeholders. Accountability is one of the most important keys to the success of a Controls Self- Assessment program. It is really important to clearly define up front who owns the process and who is ultimately accountable for it. The process owner is the governing authority responsible for training, content, and process and procedures for tools or structure by which the control self-assessment is conducted. The governing body also owns the data collected and with data ownership comes the responsibility to protect it, so access to data should be restricted to only those that need it to perform their job function. The information should also be segregated based on job function where applicable and possible.

Determining the person or persons that are accountable is one of the most significant steps to ensure the success of your compliance program. In large organizations, once you establish which business role is the best to complete your specific assessment use the same role

© 2014 The SANS Institute Author retains full rights.

across all common businesses in your enterprise. Remember, the governing authority cannot be a member of those tasked with completing the assessment. The governing group needs to ensure the staff understands that the roles of the people engaged in the process should typically not be different. These folks are the ones ultimately accountable for the successful, accurate and timely completion of completion of the assessment. This is where the accountability belongs. Each person that participates is strengthening your compliance effort because strength is in numbers and with more manpower you can cover more territory and the productivity of your programs execution will soar. You are building a small army of compliance soldiers safeguarding your company's assets which again cannot be achieved if you spend time interviewing, evaluating, writing reports and remediating issues for just a few specific groups a year.

You want the subject matter experts answering the questions, as data has no value if it is incorrect. You need to have the facts to properly evaluate the results. The manager of the subject matter expert is the minimum level of authority who should be signing off that their employee accurately and honestly answered the question to the assessment. In many cases the most senior leader has the responsibility of providing this assurance. The results of the accountability and transparency are key factors to get good data but the completion and accuracy of the information gathered falls on the site, service or organization that is self-assessing themselves. This is very important to the process and should be thoroughly covered because if ownership is not accurately assigned then the data gathered from the process is more than likely going to be incomplete and in many cases incorrect. Getting senior management's support and enforcement of the process provides you the best chance of getting the main stakeholders to view this process as an important business objective.

5.4 Qualified Participants

The individuals that contribute to the completion of the Control- Self Assessment must be qualified and subject matter experts. Typically more senior level technicians with a Certified Information Systems Security Professional (CISSP) and the business manager are involved with the process. Senior technicians normally answers the questions based on their area of expertise and the manager then approves the responses. This holds two groups of people accountable for the accuracy of the information. This will give you some assurances that you are getting good

© 2014 The SANS Institute Author retains full rights.

information and less concern if an external audit firm were to be engaged to review the controls to provide and independent opinion requested for one of your customers. This is important to the process because guessing the answer by someone who is not qualified just gives you bad information; therefore you gain nothing by the exercise. To have the right talent be involved with the process senior managements support in the enforcement of the process to be successful and consistent. Clearly communicating this message to the main stakeholder's drives home accountability

5.5 Transparency

Equally important to accountability is the transparency of those performing the CSA process; by answering the questions honestly and accurately you will be successful at obtaining good data. There must be a strong level of trust between all involved with the process. Given the chance to be transparent when answering their given controls self-assessment provides a company's staff the opportunity to honestly respond to compliance questions and report issues without consequences. It opens up communication about issues that they need help in resolving, while at the same time setting a new starting point from which their level of adherence can be measured against. The participants of this process are told there are no consequences for poor results as it is a new collaborative effort. Gulf's business leaders were praised when they shared information about their control gaps because it helped corporate to identify risk and threats that they may have not have known about. It is much more productive to run a business when all stakeholders are open, honest, and transparent about revealing opportunities to improve, however, it is expected that for all finding or gaps that a remediation or risk acceptance plan be implemented.

5.6 True Control Self-Assessment

In order to be successful at implementing and managing the Controls Self- Assessment process, you have to understand the difference between security assessment and a controls self-assessment. Many people that have never been in the processes see these as one in the same but they are undoubtedly different. A security assessment is normally is more formal in nature. It typically requires a physical visit and interviews with site personnel that manage systems and facilities. It has similar characteristic of an IT audit where all the system setting are reviewed

© 2014 The SANS Institute Author retains full rights.

from top to bottom. It can cover a number of information security domains such as application, operating system, database, network and physical security.

Who is accountable for the accuracy of the information from a security assessment is also different from the CSA process. In a Security Assessment, an experienced Information Security engineer with a strong technical knowledge performs the review. When I first started in Risk and Compliance, the process of a Controls Self-Assessment was not clearly defined. It was similar to an IT general controls audit and a security assessment combined. Granted the Sarbanes–Oxley Act of 2002 SOX was just introduced, so every Compliance manager was heavy handed with their implementation of the Control Self-Assessment process, resulting in time consuming, paralysis by over analysis mentality. A Security Assessment has its value but with the same number of resources a lot more can be achieved using a Controls Self -Assessment process.

5.6.1 Accuracy and Speed

We all know what doing more with less means and that is where accuracy and speed come into play. It is important to articulate the scope of the assessment to maximize the value of the information you are looking to collect. More than likely, you will have more than a few control self- assessments because of the different authoritative sources you are trying to satisfy. So you should have a library of questions mapped back to control requirements that you could use to perform a review. If you don't you will end up having a lot of unanswered questions which will frustrate the participants and not give you the level of detail you need to obtain to develop useful data. A schedule should be created for each assessment of the target dates for completing the control self-assessment plan should be calculated in order to maintain a reasonable pace.

5.6.2 Flexibility

The proper business personnel must be assigned to answer their CSA questions. These employees should be the subject matter expert in the areas under review. They should also be provided the flexibility of rating the maturity level of their functional areas against the controls that they are accountable to manage, You may have a few participants for different areas of the business depending on the scope of the review which is not a problem because you always want accurate information generated from the process. Stay away from the simple yes or no approach

© 2014 The SANS Institute Author retains full rights.

and focus on the level of attainment. You need to have more than two golf clubs in the bag in order to score well in golf and the same is true with a questionnaire. If given only the options of yes or no then the accuracy of the data is not always correct. In most instances obtaining the level of achievement of a certain control will give you more accurate information. I like to refer to it as the level of maturity in meeting a control. Sometimes it is the approach which will determine whether you get useful information and score or just check the box type of responses. I have found that a scale of maturity in meeting control requirement gives the person completing the assessment more options to accurately answer the questions.

I prefer the Information Systems Audit and Control Association (ISACA) rating scale, named the COBIT Process Attribute Rating Scale (According to ISACA, "n.d."). The categories are as follows: Not achieved 0-15% achievement, partially achieved >15% to 50%, largely achieved >50% to 85% and achieved >85 % to 100% achievement. I also include not applicable options for those one offs but, as I stated earlier, if you have too many answers result in not applicable, then you are probably asking the wrong control questions. You should also ask for comments for any control that are scored less than fully achieved. This will save you time later as you review the findings to determine next steps such as remediation, risk acceptance or risk transfer.

5.6.3 Tools

You can perform these assessments with spreadsheets but if a large enough organization you may want to look into and electronic governance and compliance tools. Today there are a number of IT governance providers that offer good systems with productivity features that you would find helpful if you look to automate your Information Security Management program.

5.6.4 Management buy and metrics

In order for a compliance program to have an impact on the security posture of an organization, it is important to first get senior managements support. They need to acknowledge the value of the program you are establishing and support it fully. This is especially important in large organizations that consist of many locations and entities. It is important to set up a meeting with the most senior executive within you department and ask if you will receive their backing. This becomes very important when you kick off the process with the businesses stakeholders.

© 2014 The SANS Institute Author retains full rights.

You can leverage senior managements support in getting cooperation and timely responses. If your senior management has an invested interested in the success of your projects, you should communicate that to your stakeholders and provide regular reporting and metrics by business unit for all involved.

When compliance issues are categorized and analyzed across the enterprise you will find the most common risks across its businesses repeat themselves. With Metrics, you can provide a top down summary hitting on the facts and improvement opportunities so senior managements has an understanding of the value you are bringing to the table. By safeguarding the organization, you bring value and if you bring value, you are recognized as an important spoke in the wheel. Baseline control reviews not only prevent risk they can be used to identify significant risk especially on systems that are revenue processors. Not all risks or hacks can be prevented but if a strong controls program is in place there is less of a chance of material impact on the company's bottom line. Companies such as TJ Max, Target, Michaels and Neiman Marcus have lost hundreds of millions in revenue due to security vulnerabilities that were not adequately safeguarded (Ponemon Institute, 2013).

Metrics showing improvements is a professional and impressive way of displaying data with charts and graphs right from the systems databases. There is nothing more rewarding than to give senior management a simple high level view into key areas that show the benefits of what you are achieving. Dashboards can also give your customers and stakeholders an instant view of items they have interest in regularly monitoring which can give normally results in increased confidence in your services.

In Information Security reporting, it is valuable to be able to evaluate the results of the assessment by information security categories. You will want to know what areas your organization is strong in and which ones need more attention. For example, you may see access security has consistent strong controls across the enterprise, but your encryption program needs some work. You will normally have common trends in control gaps across enterprise organizations. If you are properly using your metrics to guide your information security programs, you should see positive improvements which will justify the value of your efforts. Metrics can always be used to create some motivation for the participants. One of the best things to track is the status of all like assessments. If you can show who has completed the process, you

© 2014 The SANS Institute Author retains full rights.

can use that information to motivate others to complete theirs in a timely fashion. If one group comes up late and is behind in comparison to their peers consistently, I do believe they do need to be made aware of their shortcomings and be given a chance to get on the right path. If the behavior does not change and their lack of performance does not improve, I will contact internal audit and ask that they are put on the audit schedule. I will also escalate internally and normally plan a site visit to reinforce there needs to be improvement. I hold them accountable for this, because without the data, we do not have the ability to provide metrics, which in turn drives remediation of potential vulnerabilities that threaten the company's security posture. Anyone who is worth their salt does not want to be on a list my list of low performers.

5.6.5 Think strategically

In order to be effective on a site by site level across a global Enterprise Information Security professionals have to think strategically. You need to know what your greatest risks are and schedule time to revisit these areas of risk annually to validate that the controls are still functioning as management has intended. You should build relationships within your organization and participate as a steering committees member on large initiatives within your organization. If you are going to invest time and resources in building your information security program you should carefully evaluate your budget and look for automation opportunities so you get the best long term return on your time spent.

The right governance and security tools provide better mechanisms to cover more ground within your IT Organizations computing environments. You will be gathering a lot of data using tools, so it is very important to always keep the scope of your work in focus. Focus on the obvious issues first and gradually go deeper into your reviews as first tier of issues are resolved. Time is money and if you find a vulnerability that is glaring, you should bring this to senior management's attention. You do not want to turn into an operation person, nor should you, so you should focus on the framework and Information Security Management program and let the operations and business folks work out the remediation or risk acceptance. There should be an oversight board and senior operation management personnel involved in the review and approval of all remediation plans proposed to mitigate findings. It is important to stay focused on the goal of enterprise compliance and stay independent of the operations function. This is not only

© 2014 The SANS Institute Author retains full rights.

important from a leadership development arena that you stay focused on strategy but it also ensures that proper segregation of duties is being applied.

Continually learn and challenge yourself to improve and educates yourself in all areas of Information Security leadership. Also focus on controlling the information security and compliance program on all projects which include systems and new technologies that are being deployed in your environment.

5.6.6 Added Value

Adding value beyond the intended use of the Control Self-Assessment Process is frequently overlooked. Standardized operational practices picked up from the best performers should be cross pollinated to the lessor of the performers to limit deviation and improve overall production across and enterprise.

In today's business culture, most of us are asked to do more regularly to meet the demands. I recommend you use tools to help you achieve high results. The upfront work in building the system is the most challenging, but once you get a good tool up and running, you will have a more organized and productive approach to managing your compliance program. The cost to travel to gather information is reduced with web based systems with built in communication features and there is less need to interview if you are automated and have engrained accountability and transparency into your culture.

5.6.7 Remediation

It is important to assign the findings you get as a result of the questionnaire to the correct person. The correct person to assign a finding to is that person who has highest level oversight of the staff performing the function that was evaluated, or has been designated to handle the matter. This person does have to be qualified and is normally the most senior of the operations managers. Typically the most senior IT operations person, as well as the most senior business leader, are assigned the accountable party to lead the remediation of the finding. Since senior management has supported you in the area of enforcement of accountability and transparency of the compliance program, you should expect that operations and the business leader accept their roles and provide you with updates as the progress with their remediation efforts.

© 2014 The SANS Institute Author retains full rights.

6. Conclusion

As I have demonstrated there is a clear need for compliance to control human behavior. Throughout the decades, whether in business or in society, rules and laws have to be in place so people understand what is right or wrong. As the rule of man and business evolves, so must our ability to meet the requirements to safeguard ourselves from punishment from improper behavior.

Whether the controls exist to prevent corporate corruption or civil unrest, they must exist to measure and enforce adherence to reasonable behavior. Man must be protected from unlawful scams and business scandals. Technology and the norms of or societies are forever changing and with change we must also adapt our ability to measure and enforce compliance to ensure accountability for actions..

© 2014 SANS Institute, Author retains full rights.

© 2014 The SANS Institute Author retains full rights.

References

Butler, Eamonn (2007) Adam Smith – A Primer, Institute of Economic Affairs, London. A brief, simple introduction to Smith's life and writings

Dragomir, Dan Voicu (2009) The Accountability in the name of Global Corporate Governance.

Hermann, Claude, Johns, Walter. (2004) Babylonian Law-The Code of Hammurabi. Ancient History Sourcebook Code of Hammurabi, c. 1780 BCE Eleventh Edition of the Encyclopedia Britannica, 1910-191. Fordham University

Peavler, Rosemary (2014) The Sarbanes Oxley Act and the Enron Scandal. Last downloaded July 23, 2014 from About.com:http://bizfinance.about.com/od/smallbusinessfinancefaqs/a/sarbanes-oxley-act-and-enron-scandal.htm

Durand, A. (1912). The New Testament. In The Catholic Encyclopedia. New York: Robert Appleton Company. Last downloaded July 18, 2014 from http://www.newadvent.org/cathen/14530a.htm

Badawi Jamal Dr. (2010) Moral Teachings of Islam – The Lawful & Unlawful. Last downloaded July 23, 2014 from http://jamalbadawi.org/index.php?option=com_content&view=article&id=79:66-moral-teachings-of-islam-the-lawful-a-unlawful&catid=18:volume-6-moral-teachings-of-islam

Narro, Jame, Skeie, David. (2013) Crisis Chronicles: The South Sea Bubble of 1720—Repackaging Debt and the Current Reach for Yield. The Federal Reserve Bank of New York, Liberty Street Economics

Dale, Richard. (2014) Princeton University Press: The First Crash: Lessons from the South SeaBubble. Last downloaded July 23, 2014 from http://press.princeton.edu/titles/7835.html

Butler, Eamonn (2007) Adam Smith – A Primer, Institute of Economic Affairs, London. A brief, simple introduction to Smith's life and writings

West, E. G. (1976) Adam Smith: The Man and His Works, Liberty Fund Indianapolis, IN, USA. A short biographical overview of Smith's life, work and influence

Staff of the Heritage Foundation (2014), The Heritage Foundation: The Declaration of Independence. Last downloaded July 23, 2014 from http://www.heritage.org/initiatives/first-principles/primary-sources/the-declaration-of-independence

Adam Smith. (2014). The Biography.com website. Last downloaded, Jul 24, 2014, from http://www.biography.com/people/adam-smith-9486480.

© 2014 The SANS Institute Author retains full rights.

Scott, Robert. (2006) From Boom to Depression. Last downloaded July 24, 2014, from http://www.1920-30.com/business

Kleckner, Philip K, Jackson, Craig. (2005) The CPA Journal-A Publication of the New York State Society of CPA's. Sarbanes-Oxley Creates a New Beginning for Accountants. Last downloaded July 23, 2014 from http://www.nysscpa.org/cpajournal/2005/105/perspectives/p14.htm

SANS Institute (2014).The SANS website: Critical Security Controls for Effective Cyber Defense. Last downloaded July 24, 2014 from http://www.sans.org/critical-security-controls

ISACA (2014) The ISACA website: Cobit -Process Attribute Rating Model. Last downloaded July 24, 2014 from https://www.isaca.org/Pages/default.aspx

Ponemon Institute (2013) Cost of Cyber Crime Study: United State. Last downloaded July 24, 2014 from

http://www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6%20.pdf

© 2014 SANS Institute, Author retains full rights.

© 2014 The SANS Institute Author retains full rights.

Last Updated: August 28th, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

FOR578 Cyber Threat Intelligence	**Tysons Corner, VAUS**	**Aug 31, 2015 - Sep 04, 2015**	**Live Event**
SANS Milan 2015	**Milan, IT**	**Sep 07, 2015 - Sep 12, 2015**	**Live Event**
SANS Crystal City 2015	**Crystal City, VAUS**	**Sep 08, 2015 - Sep 13, 2015**	**Live Event**
SANS Network Security 2015	**Las Vegas, NVUS**	**Sep 12, 2015 - Sep 21, 2015**	**Live Event**
SANS Seoul 2015	**Seoul, KR**	**Sep 14, 2015 - Sep 19, 2015**	**Live Event**
SANS Tallinn 2015	**Tallinn, EE**	**Sep 21, 2015 - Sep 26, 2015**	**Live Event**
SANS Perth 2015	**Perth, AU**	**Sep 21, 2015 - Sep 26, 2015**	**Live Event**
SANS Baltimore 2015	**Baltimore, MDUS**	**Sep 21, 2015 - Sep 26, 2015**	**Live Event**
Data Breach Investigation Summit & Training	**Dallas, TXUS**	**Sep 21, 2015 - Sep 26, 2015**	**Live Event**
SANS ICS Amsterdam 2015	**Amsterdam, NL**	**Sep 22, 2015 - Sep 28, 2015**	**Live Event**
SANS Bangalore 2015	**Bangalore, IN**	**Sep 28, 2015 - Oct 17, 2015**	**Live Event**
SANS DFIR Prague 2015	**Prague, CZ**	**Oct 05, 2015 - Oct 17, 2015**	**Live Event**
SANS Seattle 2015	**Seattle, WAUS**	**Oct 05, 2015 - Oct 10, 2015**	**Live Event**
SOS: SANS October Singapore 2015	**Singapore, SG**	**Oct 12, 2015 - Oct 24, 2015**	**Live Event**
SANS Tysons Corner 2015	**Tysons Corner, VAUS**	**Oct 12, 2015 - Oct 17, 2015**	**Live Event**
SANS Gulf Region 2015	**Dubai, AE**	**Oct 17, 2015 - Oct 29, 2015**	**Live Event**
SANS Cyber Defense San Diego 2015	**San Diego, CAUS**	**Oct 19, 2015 - Oct 24, 2015**	**Live Event**
SANS Tokyo Autumn 2015	**Tokyo, JP**	**Oct 19, 2015 - Oct 31, 2015**	**Live Event**
SANS South Florida 2015	**Fort Lauderdale, FLUS**	**Nov 09, 2015 - Nov 14, 2015**	**Live Event**
SANS Sydney 2015	**Sydney, AU**	**Nov 09, 2015 - Nov 21, 2015**	**Live Event**
SANS London 2015	**London, GB**	**Nov 14, 2015 - Nov 23, 2015**	**Live Event**
Pen Test Hackfest Summit & Training	**Alexandria, VAUS**	**Nov 16, 2015 - Nov 23, 2015**	**Live Event**
SANS Hyderabad 2015	**Hyderabad, IN**	**Nov 24, 2015 - Dec 04, 2015**	**Live Event**
SANS Chicago 2015	**OnlineILUS**	**Aug 30, 2015 - Sep 04, 2015**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**