Sheri L. Wilson

Capella University

**TS8537 – Assurance Controls and Compliance**

**March 12, 2024**

Compliance and Assurance: Freedoms and Non-Existent Policies

**Background**

To establish methods for reviewing and testing compliance, one must understand the structure of the law, its application, its limitations, and how technology is related to the law’s implementation. If no system of compliance exists, then is it even necessary to create rules and compliance if law, regulation, and policy are not a part of the business or system? Even though one or more of those things might not be directly applicable, it is necessary to have an efficient tracking process, not just for compliance but also for what parts of the system carry risk. Because all are subject to the law, all must be able to implement the law or new policies quickly and effectively, but the important fact is that proof of the law's effectiveness using technology must be available, otherwise companies are forced to blindly follow, and lawmakers are forced to blindly create.

Few laws attempt to govern technology, such as the Sarbanes Oxley Act, the Privacy Act of 1976, the California Consumer Protections Act, The Healthcare Information and Portability Act, and the Anti-Can Spam Act and the outrageous number of articles in the Constitution and case law that set precedent or regulations (Savvy Smart Solutions, 2024).  The Constitution aims to create laws around justice, peace, defense, welfare, liberty, and prosperity for a "more perfect" country for Americans (The Preamble, FindLaw, 2023). The reviewer must understand that the computer is an assistive device, created many years ago by an unknown, non-famous team with an industry that works to carry out the contents of the constitution. The goal is to understand the compliance process, dynamics, and purpose and responsibility for both humans and computers and not to adhere to laws without a common process of sound judgment and authority with good purpose, knowing the boundaries and limitations of multi-disciplinary approaches to psychology, law, and technology. Compliance is not as simple as changing or updating technology because an order has been put forth or a law passed that specifically says to do something, although many companies operate this way, in a non-technologically automatic way. Some companies might use compliance to ensure certain technology is used in a certain way. The question for technology professionals as it relates to compliance is how systems are affected, as well as how they must be changed and if such changes or non-changes violate what law is in effect or must be created. Risk assessments are performed with cost estimates to determine how business is affected by following the law or not following the law, whether it is in the company’s best interest, and at what cost.

**Law is not Written for Technology**

Since compliance is a dependent and sequential process, with the law or rule being first, and then compliance, it is important to study such sequences and the order of authority and knowledge, not by our priorities, or hypothesis’ but by what has been made publicly available and is known. When a new law or policy is passed, the best approach is to conduct a law review, which is not done the same way a lawyer conducts a law review. Lawmakers who create laws have a different process for creating laws requiring compliance and do not set forth actions necessary to meet compliance in all areas. House Committee on Science Space & Tech has authority over almost all matters related to Science, Technology, Engineering, and Mathematics in multiple disciplines extending well beyond education, into business and research (House, 2024). Such oversight is a vast responsibility managed by the House of Representative’s subcommittees, without the requirement of significant and specific laws as it relates to areas of responsibility, thus meaning, there is an authoritative, political system and associated committees, but few published works of categorical technology-specific measures, bills, and laws because of their efforts. This is mainly because Technology is considered a broad category, not limited to software, and computer hardware, but also its infrastructure, and other systems that use technology concepts, such as imaging systems and more.

**Methodology**

The paper will review three laws, the implementation, and the feedback loop, including outcomes, costs, and other things considered important in business technology. It is assumed there is no feedback loop or process that the congress, senate, and its interest groups follow that ensures lawmakers and other communities understand the purpose and benefits, as well as the process and cost of following and breaking the law through non-action, or incorrect action, as well as the importance of their involvement. It is believed that people do as they are ordered and risk penalties, with the freedom to choose what they will comply with and participate in, adding to additional setbacks created by limitation and disorder, thus the reason for law enforcement, which only minimally works with Cyber-crimes, and only after the crime has occurred. Few preventative measures are used.

**Technology’s Role in Law**

Without an understanding of how to perform legal research, and an understanding of premise, precedent, and the system of order, compliance is a matter of doing what one is ordered to do, without comment or response. The question remains if companies and lobbyists are involved in the creation and passage of laws, or if the law is created based upon consumer or citizen complaints, and orders are given to the technology industry to force change. Such limited knowledge and collaboration often cause limited change, worsen the outcome, or provide an incomplete solution, especially if preventative measures are not considered and design changes implemented.

The hierarchy of order and justice is that the Technology Industry is designed to follow the law, is not a regulated industry, and is minimally involved in the legislative process. This is a problem when intelligent technology professionals see flaws where the two disciplines attempt to assert governance and control. Remedy through the courts for faulty technology is not often feasible.

**Examples of Law Where the Courts Cannot Provide Adequate Remedy**

* Anti-Can Spam Act orders force companies to implement technology change by forcing them to provide a means to “opt out;” where the technology solution was a simple button to remove contact (FTC, 2024).
* The Sarbanes Oxley Act forces companies to provide a signature line on financial documents by a specific person or persons; courts can provide a remedy in suits only after IRS audit and a formal complaint filed by companies. Technology offers limited solutions and does not review the financial process to create compliance within the financial software (SOX-CPA, 2002).
* The Privacy Act of 1974: First, it requires government agencies to show an individual any records kept on him or her. Second, it requires agencies to follow certain principles, called “fair information practices,” when gathering and handling personal data. Third, it places restrictions on how agencies can share an individual’s data with other people and agencies. Fourth and finally, it lets individuals sue the government for violating its provisions (Epic, 1994). There is no written body of proof or civil remedy within software or technology; citizens have limited means of proof, and matters are case by case: another problem of potential violation is access to fair judgment and due process of the law with no prevention or data insight mechanisms built in to notify, prove or disprove violations (DOJ, 2022).

It seems that laws are written, and companies are free to come up with their means of compliance but are not standardized, citizens rarely can obtain remedies, and courts cannot direct the technology efforts of companies. Compliance with the law does not seem to be built into the software process to prevent violation or change of the law. Ideally, laws would be written before, during, or after technology development and testing and they would work concurrently with the intent to prevent or deter legal action using ethics, compliance, and measurement. It depends on whether an unlawful event has occurred and then compliance is instituted for punishment purposes or if compliance measures are put in place to deter criminal acts or for conformity purposes for a specific goal, being lawful, ethical, and necessary. Freedom and variance are certain to cause problems when implementing or evaluating compliance, making standards a necessity, along with a tested and certified system aligned with the law using technology in an automated and tiered way of management. Responsibilities and oversight must be reviewed, created, and corrected if imbalanced, found to be ineffective, or too diverse that standards scalable across the nation or world cannot be accomplished. Lawlessness and simple word changes are proven to be damaging and more harmful than corrective action and deterrence. Relying solely on the system of law is insufficient since it would be a constant battle of what one can and can’t do and arguing through it with proof for remedy or consequence, therefore, technology must be seen as necessary to create change or serve as higher authority with intent to improve or change things for the better. Technology should not blindly follow lawmakers or other authoritative rulings without applicable tests and data to prove its case, but it should work with the Law and its makers to achieve and improve both purposes with proof of effectiveness.

Some laws seem simple but have lengthy cases where technology innovators are not involved, so there is little to no opportunity to evaluate technology and law conflicts, shortfalls, or problems, therefore included in the evaluation, must be a review of where and how technology is involved and necessary to answer the question of power, rulings, and where technology stands in the hierarchy of cause and effect, following, compliance, and request or demand for exemption for research and development. Since no technology exists that shows law and compliance effectiveness and results or costs to business and society, it’s already accepted that the two disciplines were not created together and that dually qualified professions have not engineered a law evaluation and implementation system. You simply cannot test something that does not exist, so the question is does it exist and how is it currently done? Justly and similarly, multiple, and varied approaches to reviews in technology and law, as well as different ‘approaches’ to implementation that span nationally are dangerous without leadership and standardization. Even more dangerous is assuming directives such as the “ISO” cover all fundamental legal and compliance areas of consideration or that it can be adapted to do so. If 60 million companies do things differently, with different audit processes, or are only audited on one measure, being finance, then much is lost. Clearly, because of the standard design of the internet, there is some form of automation or order, but it is unknown if it is accomplished by traditional compliance methods of collaboration with select humans of specific professions.

**Strengths and Weaknesses of Compliance Programs**

How can you evaluate the strengths and weaknesses of a program or system that does not yet exist and is varied across the world? What is known or conceptualized is what can be evaluated. There are strengths and weaknesses of a compliance program, but whose program is being evaluated? Law Enforcement, Mental Health, Education, and Computerization of Tasks, Non-Existent, but conceptual integration programs? The RDT&E process can be evaluated, but there is no singular compliance or overarching program to govern its requirements and consequences. When this occurs, the environment (called society) remains in a development and test phase, or ‘research’ phase of learning and finding works by others to improve upon or compare its efforts and outcomes. With such a vast array of applicability, compliance can only be instituted when something as proven testable and effective in smaller, medium-sized, larger, and gigantic areas, but systematic compliance evaluation of all subjects, expecting integration, requires a long-term study because of its vastness; therefore compliance only relates to what rules, policies, and laws that are in effect or created, which must be done following some regulation or other, with proof of effective outcomes.

**Research and Presentation**

The standard capstone project or dissertation format does not directly fit this type of problem-solving, explanation, background, history, and approach that is necessary to communicate and solve the problem fully but is necessary to meet the requirements of academic standards. Because *compliance* with standards of writing, using the American Psychological Association (APA), and university requirements for capstone projects is necessary, the challenge resides in being able to use a general qualitative study approach with a customized technique that can present the problem, use other academic resources to prove the problem has not been addressed, or to what extent it appears unknown, and to use it as an opportunity to explain the theory of compliance, or another complicated technology acceptance model of society’s acceptance and adaptation to what is provided in the marketplace, or workplace, in that, we use and adapt to what we are given, with few leaders in the field able to innovate and engineer a more effective product that meets the requirements of many, while protecting the prosperous endeavors of all, and the problem being that prosperity is the priority and not social or technological evolution for a more healthy nation, or community with the ability to span the system nation-wide and then globally. The current system is forceful, financially motivated, and punitive.

**Organization of Problem, Research, and Findings**

There is greater difficulty communicating the problem using APA standards, and because ***compliance*** is necessary, it is a perfect example to show how technology has progressed, while another discipline or industry profession of psychology remains the same, with one forcing its way into another. It’s one example of how non-progression or possibly regression or non-growth in one discipline (psychology) affects or stifles another (technology) and operates through education systems forcing compliance with old standards, without allowing innovation. Qualitative and quantitative analysis, tests, proof, connections, and research are possible, but it’s another round of general reviews of nothing specifically useful, to see how one process affects or integrates with another. A legal review format might be more suitable than a collective review of recent works that present generalized research summaries of compliance that cannot be applied in a standardized way. The theory is that there is no standard model for law, policy, and compliance, or that the responsibility belongs to legal professionals who can benefit from working with technology innovators to update and integrate systems. Cyber-security seems to be a field of information protection but relates primarily to securing access control mechanisms, with no specific legal process, other than refund through banks, proving security is only effective in finance and some identity theft matters.

**Current Legal Process**

The Federal Register provides information on how a law is passed, with no obvious or simple way to understand its process in steps and how and when companies can get involved or what mix of companies are selected to evaluate the law and provide proof of its effectiveness. There is no information publicly available about who the governing bodies use for their Technology to track their processes and work products, or to show that they have a well-functioning implementation system. Lobbyists for certain things or causes bring forward a bill for the passage of a law, like a request of Congress, and are passed by a vote. A law is passed and legal or compliance departments are officially notified of the change in law or creation of law. Companies are expected to comply within a certain timeframe or face audit and legal ramifications. It may or may not be solely driven by what a company is interested in, but a lack of interest could result in changes that they could’ve prepared for or prevented, much like many problems. Law and compliance are not a sales item on a shelf, but the way software services are structured, they might become or are seen as a service item for a long-term contract price, depending upon how it is structured, but companies and legal professionals don’t often know they have access to something or need something unless they can see it and there is proof. Some companies have astute law departments well qualified to evaluate the law and assist in implementation, but a standardized formal business review process, before its passage, along with its impact does not exist; therefore, companies are not offered fair opportunity to be part of the legal process; they are seen as those forced to follow, an evaluate their systems, unknown outcomes, results, and changes. This is dangerous and costly. Law software is not the solution; it requires more study of integration, to determine if it’s even designed correctly or if society has outgrown or changed its old ways of greed, instability, excessive disciplinary needs, and obsessive need for proof, accusations, truth-finding, and testing the well-established boundaries of what is considered healthy. The fact is, many people in America do not bathe and are not forced to comply with hygiene standards, and many businesspeople are not forced to comply with business rules and ethics and the sickness continues to grow, as does corruption, crime, and bad environments. There are crime statistics, but that is not enough if how it was accomplished cannot be shared or changed to promote prevention or start/stop forcing, scanning, patrolling, recruiting, working, and advertising. This gives reason for a different type of community control and allowance for the removal of citizenship, the right to privacy, and prosperity, and the requirement to force change.

**Power, Authority, Responsibility**

Who’s in charge of technology? There is not a legally qualified board of professionals in multiple areas that publicly convene and begin the passage process because it is considered proprietary trade secrets because investment and profit are necessary. Technology, unlike the legal profession, does not require Pro-Bono work and the system of law does not require integrated reports and systems for its effectiveness. Bribery is often visible or called special interest groups, or those who are impacted and can benefit, by establishing new order and justice for new areas that have no legal process. Research, development, test, and evaluation programs might not undergo a law review and are not managed by the performance systems that show the cause, effects, and shortcomings of its creations, so how can anyone know whose governance to follow, if little can be proven, or even made aware of such need?

“Follow this order and do this” works only for a little while, and eventually, corruption, problems, and other dysfunction become visible in immediate actions where results are seen. Long-term actions and empirical studies of greater impact take longer because they are wider in scope. A checkbox and signature from an official are not as simple as adding a checkbox to an internet page; it requires a full understanding of what you are signing, like contract law and all of its associated responsibilities and rules of management or use.

Just a quick review using the search terms “law review and compliance software” produced a curated list of software, that appears to have been evaluated, but no compliance or authoritative directive showing that software is approved and recommended for use. Capterra’s software center offers free-to-use downloads of over 100,000 solutions and says, “We get paid by software vendors because we help connect them to people whose ***challenges their software is built to solve.”*** (Capterra, 2024). Just hearing that challenges are “solvable” is a deterrent because it is an incorrect use of the word and seeks to promote another database of what looks like duplicated downloads larger than a gigantic city. People cannot test and evaluate them all, use different ones, and expect an integrated legal system to work effectively. The “do what you want to do” approach is dangerous and delays or prevents the creation of a more insightful solution.

One must have a law to implement or a law to check if its systems are by the law to begin, but should the intelligent and innovative be required to follow laws established by unqualified and unskilled lawmakers? What happens is that lawmakers begin to set laws and force technology companies to do things that make it more visible who functions innovatively vs. who quickly does what they are told. While it is wise to research to find out what exists and is offered or available to the public, if the law is not correctly written, then it becomes an evaluation problem that must determine who should follow whom or set the orders for what is considered “must haves or must do, how, and, or else consequence.”

Computers and software systems can be tested for compliance with and for what was requested in the discovery or requirements phase, but it must be clearly stated in the beginning, after the sale or presentation of the sale process. Defining when is challenging and companies are allowed to make their own decisions as to when and how they want to pay for their systems. This is one main problem in the way that technology is created and sold today, thus making compliance a challenge for where and when it should be utilized or created and adapted if it even exists at all. Companies are not expected or allowed to force compliance or to even make demands, yet some do, which is what is categorized as requirements and specification management, ransomware, or a faulty understanding of process, authority, and dysfunctional management of expectations. Boxed technology makes it easier to manage compliance before the boxing and manufacturing of a large number, but processes cannot solely be worked internally, and companies should look for ways to standardize processes in both environments. If direct experience with a manufacturing belt is required, then no one further is ever capable of creating or testing. A new understanding or explanation of old reference is that technologists and more are expected to “adhere” to rules and regulations, laws, and policy, but someone came along with word games and transformation, to create compliance, which might not be the best fit for all areas of technology, business, and congressional necessity. The thought that “adherence” changed to compliance, leads one to believe that old theories of subliminal messaging, mind control, and other psychological tests might be true, advertising-based, and therefore is now in a compliance phase of test to prove human control using technology. These are very useful theories and tests when proven, but can also be very damaging to humanity, thus the need for protection, independent review, management, and oversight is required, beyond simple IRB approvals or individualized psychiatric evaluations.

Understanding both internal processes and customers is required, as well as how changes affect other systems; known as integration testing. Since the technology product lines have grown, the challenge has become greater, if not impossible, creating another problem. Virality is a matter of modern influence, contact, and the means to produce a mass result and it extends beyond socialism or political structuring. The problem cycle begins to be seen as connected, replicating, or being manufactured nearly equal to the number of products on or at the belt (the multi-use term for geo-political legal battles of wrongly focused time or improper placement of the right judicial with an intended outcome for a fixed system to eliminate inexperienced human generated disaster).

Managing compliance problems in a single-scope study is beneficial, but we don’t manage compliance, and the research question is not related to management, so the scope is limited to one when there should already be a standardized compliance strategy in place. Compliance research cannot begin with a problem if compliance processes are unknown or so varied, and only available in one or two departments where there is no direct or indirect experience. Compliance is reviewed from two sides: the developer (or manufacturer) and the user of the product and its directives for compliance with the product use policies. The question remains: compliance with who, where, and based on what authority; written, verbal, and for prosecution by what level of jurisdictional power, based upon what extent and boundary or branch if it can only be generally stated? Compliance with an external body of law, or regulatory organization is external to businesses and organizations, where specific processes, or policies are created for employees and people to follow them to ensure compliance with governance. Objectives, purpose, benefits, costs, system or process changes, and outcomes must also be measured to not only comply but also understand the impact on multiple areas, even if not directly seen or written in the law.

The methodology or technique for such a test can only be beneficial and created when the specific question of compliance is well defined, scoped, and test systems are available to show valid proof, otherwise, the test, its associated systems, and outcomes remain theoretical, never proven, mysterious, and terms such as “results may vary” must be used. Since there is a standard test product test process that uses these caveats or outcomes, it’s likely to assume that the creator, manufacturer, or seller does not know the outcome, and cannot make promises because of the vast array of possibilities and variations in systems and odd connections not fully researched, or that the limited scope test cannot be scaled to other systems as a standard “approach” to achieving specific results per system test. As you see, the words, like “methodology” and approach can be standardized and categorized, with a proven process to show specific results, but nothing yet exists.

When the IT Doctorate program teaches compliance, but nothing standardized exists to follow or begin to consider reviewing, evaluating, and automating, it can be assumed that someone has “put the cart before the horse” meaning that something is improperly positioned, or that it is too soon, that something must be either created, tested, proven, with results, before it can be guaranteed or managed by the law, or under the law. If technology operates above the law, or conflicts with the law, it is not often seen because there are no technology audits and for technology to be a part of the legal process and be more effective, it must integrate with the law in ways in which it can be more useful, other than software for lawyers and the law system itself. It must be incorporated for outcomes to be seen to show proof that the law itself is beneficial and not harmful to the health and prosperity of people, places, things, and more.

A short law review shows that one inadequately directs another, or attempts to, but does not address all sides of the legal issues, and if that is the standard law process, then it can be expected that all laws created after will also inadequately address all sides of the legal issues of the system of technology. There is an assumption based on brand recognition that a user’s sense of security correlates with their knowledge of the popularity and success of technology business names (Morgan, 2023), showing less of a necessity for compliance because of their familiarity and popularity. Since the law shows that it makes attempts to be part of the technology process if the two systems cannot effectively be standardized or process specifically known and tested, then there remains either a conflict, which can be explained in many terms, or that it remains ineffective or defective or must evolve concurrently, or sequentially, understanding that adaptation is of old survival approaches also seen in technology.

Creators attempt to create within the law, considering the law and ethics, but if nothing directly applies and is not specific, then leeway offers a new system that must be developed and tested. While it is often said that there is a cost to freedom, there is also a cost to law and order. Rather than follow ideals of restricted areas (or fences and walls using frameworks) it might be best to give technology the freedom it needs to test the law for its effectiveness to show proof that the system works and then consider how technology can prevent the use of the legal system through compliance measures. Because Risk Management is a part of technology’s development cycle and acquisition decision-making (Sherman, 2022), such evaluations enable products to be certified as evaluated, rated, and trusted, yet no well-documented standard system of evaluation exists. Those who work in RDT&E and compliance must understand something is missing in the entire process and see that its outcomes are devasting when companies mix compliance with acquisitions of untested products.

This is the current situation with technology: no visible system of certification exists. How can the law be effective if there are no governing laws applicable to the RDT&E or acquisitions process in both government and commercial systems? If the law proves to be inadequate, then compliance efforts will also be inadequate for existing systems and one cannot effectively direct the other and serve the people. If the world or industry has a global or national strategy and plans to implement cloud computing or a new design, then it is suggested, based upon the use and explanation that “results may vary” that they should know and listen that compliance improvements can and should be made or shouldn’t be made concurrently, or not at all because sequencing is a necessity. There is no existing methodology, thus a new one is created for this area by using three law reviews. It must be known that the law serves the purpose of disciplining and creating order. Technology has the same purpose, without punitive or disciplinary structures addressing all parts of its design. One cannot rely on old laws, and ways that once worked when it has new technology; both must evolve or adaptation is required; and to implement without measurements that span beyond the stock market, or financial outcomes is dangerous and of no added value to society’s improvement.

**The System of Law and Technology**

They are incompatible because if the law is going to pass laws for the people and the technology companies do not follow it, and know more than the legal profession, then the lower authoritative power creates more problems and operates uselessly, potentially setting itself up for its own disaster. Class action lawsuits against companies are also not the answer because Technical Investment and Direction is a better place to direct for prevention, but the law cannot technically direct something it does not know or is presented with high-risk warnings and constant threats and violence, such as guarded facilities, corporate foreign entities, and low-quality innovators that sell street violent-tendencies, cops and robber games, while working to better society or understand how gaming affects real life in virtual physics. Keeping it unprovable, profitable, and exempt from the law is their strategy and money is their tool.

*Rather than developing constant contact (an email advertising and newsletter business software suite), it appears society, law, and technology, are now in constant conflict, after review of the Anit-Can Spam Act.*

**Compliance Originates from Discipline (Parental, Military, Law, Corporate)**

Currently, what looks like military protections, directions, and executive oversight and investment might exist, it is still unknown if the creators are in the US Military, which looks like a prison, and plan to create more prison-like systems, locking businesses and people into faulty systems or more abusive and failed approaches to improving what exists or creating a necessity; if compliance proves to be a necessity, then we continue to function in a cycle of war and peace, where order is maintained by what many report as a corrupt system. If it is a cycle, and technology, along with the military can create improvements or social change, then civil war must be a consideration. Just as we are unsure if the US Military is a prison itself, acting by itself, and knows nothing other than barbed wire fences, handcuffs, and punishment in law, then technology does not know if it can create safety measures using an existing system of recall, or if the result in theatrics, because of the political system depicted in “Total Recall.” While military prisons exist, it is a separate and different judicial system that has one law that prevents another disciplinary action called “Double Jeopardy” which should never even be considered since its counterpart is a game. Jeopardy is a perfect example of a design that goes against English and common standards of question and answer: The answer is provided, and the correct response is in the question. Technology or code is different than the English language. Since the process is not created using single subject or sentence structures, technology cannot be subject to the Jeopardy or Double Jeopardy legal processes, unless it can systematically result in the same number of questions and answers, with a random selection process and it is clear, in your eyes that questions and answers are not contained in boxes, yet we have process systems that are used to place process information in boxes. If ignorance comes along using animals in boxes to test its theory, then it could result in no response at all if animals do not have a process for how they do things or are undocumented because it is assumed that humans create processes for their animals in training phases; and animals have proven themselves to be non-domesticated, untrained, superior, reliant, and inferior to humans. The same type of relationship exists between the Law and Technology.

**One or More Complying with Bad Leadership, Creates a Bad Population or System**

Duplication of bad behavior, crime, and intent were reviewed, but technology tests proved incapable and irresponsible people were creating systems, provided, and created by others, following other bad leadership, accepting low-quality technical products, or only what could be created with what was provided in training. Results may vary still, as do threats, without deterrence programs, creating an environment and inability to comply or operate in specific environments because of such improper treatment. The results or findings and perceptions might be summarized as a “bad idea” “bad business” or “faulty system” or as impossible because of the past, or present conditions, in which we live our lives in goods and services contained in contracts. If all people are legally bound to contracts, and those are bound by the law, then does a bad contract result in a bad product or service? The answer seems to be only “slightly” available for honest proof, without specific standards of test in law, ethics, and documented results. Some go insane for their need of documented proof, while others go without their essentials just for working in technology; an odd sense of power imbalance or difference in ability – leads us to a system of order and question, if the whole thing is “**just** out of order” – another standardized term used for coke machines, of which the law seems to think we are the creators of and can and will do similarly to feed their sensational appetites for risky and unlawful behavior or false assumption that change is required in both silver and dramatic gigantic worldwide systems that uses change management and multiple forms of currency. Understanding that all senses are working, available, and functioning, many who make/made decisions weren’t, with the law operating only on “alcohol and controlled substances” being its only concern or understanding of “impaired” results. Merging, pairing, and integrating are different acts or considerations, not done concurrently with box checkers and low-quality incompetent evaluators. We are box checkers; providers of data to companies who are not forced or bound by the law to share, therefore we remain protective, guarded, and unnecessarily questioned. We live and work in square and rectangular spaces, have various standards of living, expectations, and behavior, and our inputs and outputs are also in boxes, of metals. We drive cars of different shapes and materials, and our clothing, religious beliefs, income, family dynamics, and education levels define our life’s functioning, confined to spaces and places for a specific purpose, not always of choice or pleasure. Strength in numbers overwhelms and vast differences cause disfunction, proving world disorder, and disaster areas, where mere functioning has become a life of questionable conformity to expectation and the system of professional work.

Some do not know the difference between their motorcycle and humans and the order of importance in investment, yet continue to be funded, awarded, and individually allow their hands, feet, and mouths to accelerate, claiming technological backgrounds, and parts reaping only rewards while causing failure to the lawful, correct, and valuable ones who were and are disciplined, corrected, trusted, evaluated, and given power and authority to create. Financial and mental imbalances showed severe monetary and incorrect affectionate outcomes in humans, blaming it on the computer; that the computer could not feel; resulting in thousands of dollars more towards human insult and dysfunction to support and “portray” themselves non-theoretically and theatrically on laws of manifestations and air disasters, as well as severe “bugging” of nature’s insects, animal and other predatorial and territorial attacks occurred, still not knowing the purpose, source, other than that “she, they, or them” had no compliance department and misused and mistreated the right professional that could’ve prevented them from hurting many others. Are we still paying for the Vietnam War? No, but we are still suffering from problems with Asian American citizens and workers allowing, restricting, or not restricting internationalism or human cloning and blindly forcing or demanding human kindness and diversity. Human forgiveness and debt cancellation, or bankruptcy takes a long time, and some things simply cannot be forgiven, especially if the law fails to do its job.

**Does Everything Require Law, Policy, and Compliance?**

Humans began to collect and display animal parts in jars inside and outside their homes, theoretically, because there is no law on the Food Pyramid or dietary pleasures, it is only ***suggested*** by the US Government. There’s no specific law for the morgue in catering to odd orally pleasing pleasures, resulting in another legal problem extending to those scrutinizing the law and actions of another, attempting to utilize name calling, declarations of sexual use, policy, and law; separating the two, resulting in vehicle crashes without consideration of ethical responsibilities or traditional behavioral expectations and differences between men and women, and the potential computerization can bring and because of incompetent leaders, failed to so do. If one is being told, trained on a process, and follows a standard of order and discipline, using statistics and becomes one of the statistics and the other is not subjected to the same outcome, then it is unfair, unequal, damaging with no legal remedy, but this just proves more deficiency in the system of man, woman; either discriminatory or non-discriminatory based on expectations and teachings of someone else’s findings necessary to show proof, despite safety.

The laws cannot be followed if basic human ethics are missing, yet, the ethics could be followed if the lawmakers were ethical, and this is just a short review of the “transference” with and without interference, considering the loss and movements of others, without regard to the unnatural and dysfunctional conditions under which one or more was forced to work.

Information security standards were developed by NIST to further its statutory responsibilities under the FISMA Act. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems. While it works for financial transactions, such standardization is missing, and no one seems to see the necessity for improvement. This publication provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks. Banks operate in a highly regulated environment, and accurate knowledge of dependencies is vital for ensuring compliance with regulatory requirements, such as data protection and business continuity planning (neo4j.com, 2024). Developers published a dependency mapping system, for developers, which seems it would be better and safer to publish something non-technical to show which regulations govern what requirements for data security and transacting, showing requirements, rather than technical code that won’t ever be directly used because of the way financial products are now designed for e-commerce. Such publishing requires scrutiny because it is honestly not reusable code or valuable understanding in how compliance standards are correlated to regulation and offers no real benefit if the final answers to all are: it depends.

**Comply or Defy? Do it or Else.**

Why even bother if there is no system, standard, or effective outcome or there is but it is so farfetched that dogs are now the priority and humans? There are only a few differences between a Mental health facility and Doggy Daycare Kennel, showing the treatment of humans and dogs being closely and wrongly functional, acceptable for some to span across the United States with profitable and high-cost healthcare and pharmaceuticals. Unfortunately, inhumane treatment has already been proven to have been inflicted and still lingers as a future home or result of efforts. Not only are animals mistreated, with no obvious activism or change, but humans continue to be also; while America’s healthcare only mildly cares for the sick and injured, closely mirroring law enforcement’s correctional system with no effectiveness measurements; only statistics to prove healthcare decline and financial troubles. Technology enabled this to occur, and technology can shift it from being an ongoing money maker through business management and law changes, not done by vote or, poor governance, or civil choice.

**Compliance is reviewed with caution, Post objection because of Threats and Damages**

One governing body passes a law for some reason, a need to protect, deter, or prevent because there is a risk in some area. The Individualized Privacy Policies and Privacy Act of 1974 is the best example of this as it explains problems with the implementation of the law using a one-to-many regulatory structure. To simplify the problem, the Internet contains many businesses, or legal entities, some registered with the government, some not, and some using the federal banking system, or gathering and using personal information.

**Compliance and Conformity: Creators of Limitation**

Originally, people were cautioned and threatened, forced to do business with whom they “think” they could trust, or those that appeared to be trustworthy, often marked with some seal or protection visual, such as a lock on the HTTPS:// address block, much like the human housing system, but with a visual and proof of good business. People were also forced to forgive, without judicial intervention, damaging a large population. People were expected to learn this and use discretion, and naturally, with such a large population, feelings on use, as well as activity, varied, but the business procedure for collecting, storing, and using information was somewhat standardized, non-visually, but in data specifics of what was or is used to transact. The same is true for the ways humans develop personal relationships and trust; in some cases, it is automatic, until something diminishes it, either through education, learning, or experience. If technology is different than humans, then the system should be designed differently, with the correct validation and compliance methods built in.

The same problems exist in incorporating other cites/sites within the methodology, or the search for other understanding and proven results on something that does not yet exist or was removed because of damage.

There are federal laws protecting the information, and a standardized process for using banking and credit cards online, and the same approach is or was taken to protect personal information, even if no money is used. These were technical standards with an accompanying law to ensure businesses followed and to instill a sense of protection for citizens or internet technology users. It is unknown whether the law was created first, or the system was created per the law, who set forth such regulation, or its review and technology change system. It is justly known that when a law is passed, internet businesses are required to conduct systems checks and ensure compliance. Few laws have been passed that direct the internet conduct of citizens.

What technology companies and businesses have yet to realize is that standardization and modern technologies can create systems that are compliant upon installation and that customization to their business name, and process can be created for their unique products and services. If technology companies were to take on greater responsibility in building in legal requirements, such as information sharing and use protections, reports, standards, and federal compliance processes by programming it into the technology before release, then businesses would be relieved of the legal responsibility, making it easier to manage, using technology and rapidly changeable from upgrades at a regulated price on a regulated and manageable schedule. A simple example is the Privacy Policy where each company on the Internet must have a privacy policy published on their site if collecting personal information. Internet site designers and application programmers create one for the business they are working with, which produces variation in policy since sites are not automatically created. There Are Between 12 and 24 million Online Stores (The Social Shepard, 2024).

Such variation now passes on risk to the consumers and forces acknowledgment and legal understanding of the use, and such standardization creates manageable automation. E-Commerce was accepted by its users because it only mildly differed from the physical credit card process, which is a contract with specific terms, policies, and agreements. By making it similar, technology lost an opportunity to standardize its contracting process and how it manages, delivers, and receives information, giving way to fraud and mismanagement on both sides of the business coin. Insight into data with special features changes this practice, while some argue compliance and law, or law enforcement change it. Non-standardization of the law, policy, and various ways of explaining creates disorganization and leads to mismanagement, which leads to breach, potentially to the point where people ignore the policy or click through it without reading and trust is automatic because the need or want is greater than the perceived risk. The problem is that now that the Internet is accepted as a trusted source, cybercrime still exists, and trust changes, affecting economics and more. Awareness and training change, as do buying habits, and naturally trust and pleasure increases or diminishes. The understanding of the availability of pre-programmed legally compliant and protective systems must be accepted as real, possible, and not currently offered, are managed individually, and only recently have companies begun to work together sharing authentication data to make personal account management more efficient. If a governing, regulating body, or consumer has less to manage, the more effective they would be, but because each company and person is free to create their own and do business on the Internet, or pay another company or person, the law is managed and policies created using a one-to-many ratio, without automation and no compliance tracking. If there is no compliance tracking using automated technologies, then there is no way to forecast, prevent, deter, or ensure the Internet is working as a safe information exchange. Freedom has cost each company, forcing them to be held responsible for their operations, legal compliance, and protections, and the burdens are passed down to each user, sadly, when technology can program into its standardized designs necessary items, or better organize them for consumer protection and awareness.

For example, the Consumer Protection Program could be formed to contain one privacy policy that all businesses agree or are forced to follow or comply with, to protect its customers, and applied to business-to-business models to protect both sides and ensure fair competition to reduce deceptive and unethical practices, but no such agency exists. There are potentially 12 million or more internet pages covering company Privacy Policies. A consolidated standardized policy could reduce it to one or two, or a single regulatory agency with manageable terms, specific to its parties. Discipline and money cannot be the top necessity or quest in life, nor can they or social collectives, gatherings, and individualization govern everything, yet it does, for a set time. Poverty penalization has already occurred because of the earnings system we are forced to comply with and without opportunity, we have social dysfunction and more. With bad business and non-technologically correct leadership with time and money, we end up as housekeepers of a multi-disciplinary problem that could take just a few days to change but are forcibly disabled and reach a point of complete disinterest, ultimately leading to withdrawal, non-completion, or another unachieved goal.

Failure to follow one direct order or failure to state it was a direct order resulted in the loss of millions of lives; all seemingly necessary for American and International Prosperity and Peace, but resulted in severe economic and human physical and emotional disaster, unrecognized in many areas because decision-maker and leadership failed to empower a single individual to make decisions in the best interest of the entire world: An international government structured disaster that went from learning and earning in the non-traditional family system, while forced to comply with irrational demands or faulty commands. Compliance and force must have limitations and immediate removals to prevent continued ongoing life and information disasters, beyond technology. This paper presents a larger view of human psychology combined with technological endeavors based on five or six senses, with the chance we might need to venture into the development of more without trying to find the secrets and solutions behind power imbalance and misuse. Much has been established and published that cannot be lost and requires careful consideration before changes can take place and sometimes prioritization of needs, wants, and outcomes cause problems.

**Integrated Governance with a Decentralized Technology System**

Who or what entity or agency? What politician, lawyer, or lawmaker? What citizen, leader, or person? What paid spokesperson, professional paid and qualified or unqualified and paid or volunteer professional? No centralized site for regulation, policy, remedies, or personal management exists in all lives and professions and it likely results in courtroom overflow, lengthy or no trials, and loss. One could argue that the Internet provides all that and more, but using a single-site approach, a one-by-one implementation model, and not an automated legal compliance system that defines and outlines its scope, purpose, and benefits, enabling technology creation to prevent and eliminate unnecessary requirements. Redundancy in data use and storage is also an issue using that approach, as is the management of variations of law by geography, state, industry, monetary value, or even demographic.

To view compliance on a task-based level as to what laws and regulations apply to specific work fields, such as finance, information protections, and consumer protections is well intended, and useful for companies and organizations that operate effectively, but causes a great deal of dysfunction if left solely for human compliance and internal verification, leading to the only visible result being a financial document or efficient internal business process; operating on goods, services, and information exchange similar to physical commerce. Compliance is related to behavioral management, but is different when it relates to computerized systems, where a different approach must be taken. Compliance programs can check and ensure security is compliant with regulations; but each area differs; making no real standard, as NIST says, beyond a password authentication system, or physical security measures of computer systems. Complete consumer protection and business security can never be fully reached if each must manage its own and be accountable for every standard, compliance process, and single or multiple governing bodies, as well as any civil liability that arises from doing business, forcing the necessity of a legal professional or paid advisor just to do business. This leads to limited opportunity, yet the freedom of the Internet enables anyone to learn, create, and sell, with little to no oversight, audit, or advanced training, which leads to lower-quality and varied e-commerce systems, especially if one party decides to automate protections and compliance using built-in technologies, then industry faces the same challenges that the socio-economic stratification presented; access to opportunity at varying degrees of cost, price, quality, responsibility, and risk.

We have the technology able to provide users or businesspersons and consumer insights of value, yet no one company has come along that can consolidate, monitor, protect, and validate information, or make its management more centrally efficient. The current design brings freedom, but much knowledge is required, and more responsibility and risk, duplicating the design of American business, far beyond finance with no knowledge management system and engineering leadership committed to its improvement.

In conducting a literature review in hopes of finding other written discoveries that dissect the problem, it is found that a wealth of studies exist on cyber-security, current approaches to security, risk management, user feelings, and more, but no research exists that explains how the architecture of a one to many design and standardization of internet protocols and automated pre-programmed requirements for the protection of national security information exists. The research that is referenced is used to show with greater strength the opportunity that technology presents in lowering risk, by showing where and how it is transferred, and placed, and what strategies companies, perhaps are forced to use to gain and retain internet customers or participation, as well as undocumented, or non-technologically specific directives that govern E-Commerce standardization. Technology has the power to eliminate cyber-crime, or at least provide a rapid means of resolution and change, and presents a great business opportunity for security companies, but society, its regulators, policymakers, leaders, and businesspersons can benefit more from a pre-programmed system that meets legal standards before its sale or approval for use, but it requires business process innovation and law reviews to make the best of use of such investment in technology.

The result could be the exemption of the United States Constitution and its legal system as it pertains to the law because the law operates using a different type of system, which is incompatible with technology, or that technology can reduce the need for heavily documented law and policy governance, by having served its great purpose in establishing and setting forth social and economic order, now capable of commanding or directing technology to produce protective systems that are pre-programmed for compliance, specific to the set of changeable laws for each region. It can be proven that legal requirements can be programmed into a system, along with standardized policies and procedures, yet it is unknown as to why we continue to operate with the current design. By being limited to only two methodologies or approaches to present the problem, much is lost, so the technique will change to using qualitative methods of interviewing a sample population to grow in understanding technology professional’s knowledge of responsibility in adherence to law, regulations, and policy as it relates to the delivering technology as a secondary item to a recommended technical approach for making technology more efficient, reducing risk and burden.

The purpose is to prove that there is a more effective and efficient design available, as well as the ability to build compliance mechanisms while solving other major problems technology presents and faces. But first, it's important to understand that forcing compliance or adherence to laws using a deficient, or minimally satisfying system, knowing that we have greater capability and that there is a better solution is equivalent to a potentially successful endeavor of controlling attitudes, beliefs, behaviors, and the functionality of a population while enabling and limiting growth and progress. A punitive approach to innovation depends on who the leader is, and proof is not necessary to see flaws and damages. Rather than consider how the necessity for law changes because of technology capability or redesign, knowing that one affects another, and could be better positioned to produce better results. Since Internet Systems design, programming, acquisition, and use are limited to only a few perspectives using a task-based approach, it would benefit the learning experience to collect data in support of a new type of programming model that is not keyworded, based upon words like “assurance, trust, policy, compliance, law, commerce” but encompasses all critical areas of information management for global strategic purpose, prioritizing national and personal security, while understanding the responsibility and challenges faced by users, businesses and organizations across the world. The goal is not solely to explain the understanding, but to provide a solution.

**Interview Questions**

The purpose of the interview is to collect data on technical professionals’ knowledge and experience implementing or changing technology *in response* to a law or act, to find out how they receive the law or policy, who or what creates local or organizational policy, how compliance is measured and to whom and how it is reported. It will also attempt to identify benefits or challenges in technology and implementing the law. Since it is not a survey questionnaire, the discussion could lead to other important areas of consideration that add proof that there is a standard model for the implementation of law and policy and that the technology process is not automated. Methods of policy creation, based upon the enactment of law, and process change procedures will be discussed and measured for variance. The interview will also inquire about and acquire professional knowledge and experience on individual site-by-site change and implementation, perspectives, and perceptions or opposition to a centralized information policy and compliance system to gauge current use and readiness for the use and validation of automated information. Questions regarding cloud computing and its comparisons will also be lightly discussed as they relate to compliance with specific laws and what professional technologists in businesses believe they are bound by or must comply with. The overall purpose is to assess if businesses are or were damaged or are flourishing from technology and if they are even aware of the design flaws.

**Population**

Professionals in technology will be sought after for interview, for those who are employed as buyers, e-commerce managers, business officers, corporate counsel, and compliance department staff. The population must somehow drive technology change and set policy or receive technical direction and utilize technical skills because of the legal requirement, to understand the communication dynamic and challenge of the two disciplines being separate or together and to identify common levels of responsibility, process, and challenges. Some data sampling will occur if commonalities exist, and information can be quantified using statistics. Interviews from at least 20 qualified government agencies and companies of varied sizes that utilize e-commerce as part of their main source of information processing are required. Simple random sampling will be used.

**Conclusion**

The necessity for qualitative and quantitative data has become an institutional matter of compliance with psychological standards or formats. This proves, that although technology offers more advanced organizational ways of managing information, sources, and stylings of presentation, institutions rely on old requirements; and the system of law does the same thing. Until the disciplines can effectively work together, loosening requirements, licensure, and test measurements, the world or the ‘technologically skilled and innovative” with capability is forced to conform, even though there are better ways of doing things. This is compliance and the effects are creative limitations for uniformity purposes. We do not work in uniforms. Because of the necessity (by some) for proof, official records, documentation, reports, numbers, and more, life becomes interconnected, and reliant on others, even though it has been observed and determined to be an inhumane punitively damaging system based upon punishment and reward or ‘award,’ rather than healthy living, innovation, evolution, change, and betterment efforts for many. The simple solution is for the law to stand down and learn its place or find a new one, along with others, and to function with a more open mindset, unless they too are forced into systems of compliance; a compounded problem of old tradition that no longer serves a real purpose. When such compliance efforts are seen as restrictive and new technology is available to improve things, but compliance stands in the way, the purpose must be known, and it must extend well past “because I or they said so.” Reason also must be known, otherwise reasoning becomes skewed; based on assumption, not proof, or no ability to find proof for new measures because the old non-proven ways linger without efforts or potential for distinguishing marks of societal change. High marks are not temporary, but are expected to be applied throughout and continued, not solely in recognition, or singular achievement for self and outward praise, but because of the potential and necessity it brings in advancing society by the discovery of power and authoritative imbalances or wrongly structured, and disordered designs.

**References**

Preamble to the Constitution, Findlaw (2024), accessed from the Internet at   
https://constitution.findlaw.com/preamble.html#:~:text=The%20preamble%20is%20not%20actually,more%20perfect%22%20country%20for%20Americans on March 12, 2024

IT Policy and Regulation, Savvy Smart Solutions, LLC, (Wilson, S.L.), Jan 2024, accessed from   
 the Internet at https://savvysmartsolutions.com/policy-and-regulation on Jan 24, 2024

Morgan, J. M. (2023). *The Role of Big Tech in Providing Cybersecurity to End Users: A   
 Qualitative Case Study*(Order No. 30317840). Available from ProQuest Dissertations &   
 Theses Global. (2817936793).   
 http://library.capella.edu/login?qurl=https%3A%2F%2Fwww.proquest.com%2Fdissertations-  
 theses%2Frole-big-tech-providing-cybersecurity-end-  
 users%2Fdocview%2F2817936793%2Fse-2%3Faccountid%3D27965

Committee on Science, Space, and Technology, House, accessed from the Internet at   
 https://science.house.gov/hearings on March 13, 2024

Capterra, Compliance Programs Software (2024), accessed via the Internet at   
 https://www.capterra.com/sem-compare/compliance-software/?utm\_source=ps-   
google&utm\_medium=ppc&utm\_campaign=:1:CAP:2:COM:3:All:4:US:5:BAU:6:SOF:7:Desktop:8:BR:9:Compliance&network=g&gclid=Cj0KCQjw-r-vBhC-ARIsAGgUO2BEBDcHZvQGHnM8kIDqawPO22VgT8CyyIGNKHbPqj9DN\_rSNlC3h4MaAp2fEALw\_wcB on March 12, 2024

Risk Management for Acquisitions, Department of Defense (DOD), (Sherman, J.B), 4/19/22, accessed from the Internet at   
 https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/851001p.pdf

on January 10, 2024

Anti-CanSpam Act, Federal Trade Commission, accessed from the Internet  
 at https://www.ftc.gov/business-guidance/resources/can-spam-act-compliance-guide- on   
 January 30, 2024

Sarbanes Oxley Act, SOXCPA, 2002, accessed from the Internet at https://www.sarbanes-  
 oxley-association.com on February 10, 2024

The Electronic Privacy Information Center (EPIC), The Privacy Act of 1974, accessed from the   
 Internet at https://epic.org/the-privacy-act-of-  
 1974/#:~:text=Access%20to%20Records,and%20make%20copies%20of%20it. On March 12,   
 2024

Department of Justice, Privacy Act of 1974, as amended, 5 U.S.C. § 552a, DOJ, 2022,   
 accessed via the Internet at https://www.justice.gov/opcl/privacy-act-1974 on March 12, 2024

NIST Special Publication 800-53, Revision 5, Security and Privacy Controls for Information

Systems and Organizations, National Institute of Standards and Technology, (), 12/20/20,

Assurance, Privacy, Confidentiality, Control, Personally Identifiable Information, System   
 Security

Federal Information Security Modernization Act (FISMA), 44 U.S.C. § 3551 et seq., Public Law   
 (P.L.) 113-283

IT Security Diagnostic Program, InfoTech, (Info Tech Research Group), 2024, accessed from

the Internet at https://www.infotech.com/benchmarking/it-security on 1/29/2024

Dependency Mapping System, Neo4j Developer, accessed via the Internet at neo4j.com on   
 March 12, 2024

21 Essential eCommerce Statistics You Need to Know in 2024, The Social Shepard, accessed   
 from the Internet at https://thesocialshepherd.com/blog/ecommerce-statistics on March 12,   
 2024

Gerard, Joseph A., and Curt M. Weber. 2015. “Compliance and Corporate Governance:   
 Theoretical Analysis of the Effectiveness of Compliance Based on Locus of Functional   
 Responsibility.” *International Journal of Global Business* 8 (1): 15–26. https://search-  
 ebscohost-  
 com.library.capella.edu/login.aspx?direct=true&db=bth&AN=101746102&site=ehost-  
 live&scope=site accessed via the Internet on January 24, 2024

The Cybersecurity Framework as an Effective Information Security Baseline: Qualitative

Exploration, Capella University, (Troia, Vincenzo), 2018, accessed from the Internet at   
http://library.capella.edu/login?qurl=https%3A%2F%2Fwww.proquest.com%2Fdissertationsthes  
 es%Fcybersecurity-framework-as-effective-information%2Fdocview%2f2126637538%2Fse-

2%3Faccountid%3D27965 on January 24, 2024

Corporate governance and the information system: How a framework for IT governance   
 supports ERM, Bradford Vol. 14, Iss. 3,, Rubino, Michele; Vitolla, Filippo.

Critical success factors (CSFs) for information technology governance (ITG), International

Journal of Information Management, (Alreemy, Z., Chang, V., Walters, R., & Wills, G.),   
 2016

No Relevant or Formal IT Regulations, Google Inc., (), 1/15/24, accessed from the Internet.

at https://www.google.com/search?q=IT+Law+and+Policy#Capella University 2023\U2A1 on   
 January 24, 2024

2022 Consumer Privacy Legislation, National Conference of State Legislature, (Greenburg, P.),

6/10/22, accessed from the Internet at https://www.ncsl.org/about-state-legislatures/2022-  
 consumer-privacy-legislation