



**LORICCA**  
RELIABLE TECHNOLOGY SOLUTIONS

**INSIDE THIS WHITEPAPER:**

Readiness Assessment	2
Compliance Gap Analysis	2
Risk Assessment	2
Implementation Plan	3
Remediation	3
Ongoing Monitoring	4

# *Six Steps to Compliance in IT and Information Security*

**Michael Whitcomb**

President

Loricca, Inc.

[mwhitcomb@loricca.com](mailto:mwhitcomb@loricca.com)

813-600-3005

1118 Nikki View Drive

Brandon, FL 33511

There are many federal, state and municipal regulations that have been enacted for the purpose of protecting individually identifiable information and sensitive business data. The various legislations are concerned with information transferability and call for better standards to facilitate the electronic exchange of information to make financial and administrative data transactions more secure and efficient. The basic underlying principles are: (1) consumers have rights and control over the release of their sensitive information; (2) the use of this protected information ought to be limited to very specific and 'need-to-know' purposes only, with few exceptions; and (3) accountability within the system; the regulations include specific federal oversight and penalties for violating an individual's privacy rights.

Many of these processes must be integrated and implemented into your business. This process can be simplified into six steps (or phases) that facilitate the result of ongoing Compliance. Those steps are:



This white paper will discuss each step and what must occur. At the end, some suggestions are provided to get your organization started toward compliance and better IT Security controls.

### 1. Conduct a Readiness Assessment

***A readiness assessment reviews three areas of an organization:***

- *Contractual Agreements*
- *Business Practices, Policies and Procedures*
- *Systems and Applications*

A thorough readiness assessment examines all current contracts and agreements with other individuals or organizations that may be considered to have a "Chain of Trust". Critical or sensitive (*individually identifiable*) information provided to you in order to perform your business must be released to you through a contractual agreement from the organization that obtained the information.

The current state of the Business Practices, Policies and Procedures must be reviewed for the entire organization wherever this type of information is exposed. This includes both written and non-written policy and procedures.

Computer Systems and Applications must be reviewed that maintain or transmit sensitive information. They are assessed for their ability to restrict the information to a "need to know" basis, as well as audit trails for access violation. This includes aspects of data storage, networks, transmission, software design, encryption, password protection, system backup, disaster recovery, physical location, etc.

### 2. Develop a Gap Analysis

Information gathered from the Readiness Assessment is compared to the applicable regulations and industry 'best practices' on a detailed basis. Once completed, a Gap Analysis will provide a detailed list of contracts, Policies and Procedures, Computer Systems and Computer Applications that do not meet these standards. This includes current contracts, procedures or systems that do not comply as well as areas of the regulations for which the organization does not yet have contracts, policies, procedures or systems.

### 3. Develop a Risk Analysis

Senior level management action against the risks will be required to determine which risks can be reasonably resolved and which risks do not apply to the organization.

Some regulations are written so that reason can be applied to mitigating the risk against the cost required to remove the gap (*remediation*) within an organization.

***Two questions are asked for each violation identified in the Gap Analysis:***

- *What are the options and associated costs for making the change to reconcile the violation?*
- *What is the risk to my organization if I do not make the change?*

### 4. Develop an Implementation Plan

Deficiencies that are determined by Senior management as worthy of mitigation/remediation are the foundation for an implementation plan. The implementation plan includes a list of tasks and activities, deliverables from completing the tasks, required resources, estimated costs, and a timeline for completion. Resources can be in the form of current employees, contract individuals, software products or hardware products.

### 5. Implementation

Once a plan has been established, resources are gathered to implement the required change. Depending on the size of the organization at least one project manager will be required to assure timely progress and to manage problems as they arise. Resources may come from multiple areas of the organization. Changes may likely impact Information Technology, Operations, Human Resources, and Physical Security. The amount of change necessary will be determined by what is reasonable for the size of the organization being evaluated.

Once an organization is in compliance with applicable regulations and widely accepted industry best practices, the amount of resources necessary to maintain that compliance will be greatly reduced. Therefore, it is most likely that an organization will utilize outside resources to perform the assessment and implement the change. Once implementation is completed an organization can assign the role of compliance to a responsible employee.

### 6. Ongoing Monitoring

**Maintaining Compliance with applicable regulations requires two activities:**

- 1) Monitoring the adherence to current policies and procedures
- 2) Modifying policies and procedures to conform to any changes in existing laws or new regulations

Having a procedure in place does not reduce your risk of liability unless you monitor the activities of the employees who must follow your procedures. Once policy is made, it must be communicated, monitored, and actions taken for violations. If an employee violates company policy and employee training was not documented, then the employer's liability will be greater than it would be if training were documented. Likewise, if an employee is allowed to continually violate a compliance policy without action, the employer's liability will be greater than if appropriate actions had been taken.

As regulation policy changes, your organization must review and revise (if necessary) their practices or policies to meet those changes. Most software vendors will automatically adapt to changes in the law; however, since 70% to 80% of compliance to regulatory laws is based upon company policy and procedures, each company will have to maintain an ongoing awareness of any changes in the applicable laws/regulations. They will have to update their policies and procedures to adapt to changing requirements.

### How to Get Started

Any organization is going to have to provide a commitment of funds, time and resources for the regulatory compliance project to be successful. The task may seem overwhelming at first because the regulations delve into almost every aspect of an organization. Performing the Gap Analysis alone can be a daunting task due to the volume of the regulations. For example, in one legislative Act, just the Privacy regulation is over 800 pages, and this does not include the Security and electronic data interchange regulation components.

The difficulty with compliance is that no one solution fits every organization. Any organization determining a need to comply with the applicable federal regulations has many options to perform the six steps listed above.

In order to evaluate your current business against the regulations you have many options including one or more of the following:

- Outsource your office and IT management to a regulatory compliant organization
- Create an Internal Employee Compliance Officer Role
- Contract for assistance in becoming compliant
- Contract for ongoing Compliance Audits/Reviews

### Getting Started - Work plan

- Determine a team strategy that makes sense for your organization.
- Identify your team.
  - Empower an employee to be the Compliance Champion (and maybe a separate IT Security Official or Chief Information Security Officer – CISO).
  - Obtain consulting services if needed.
  - Establish a project manager.
- Establish a budget.
  - You should estimate for steps of assessment through an implementation plan.
  - You will need to provide a new budget for implementation.
- Begin gathering information that must be reviewed.
  - Gather all current contracts between your organization and others (including consent forms) for legal review.
  - Gather all written policy and procedure manuals.
  - Document all unwritten policies and procedures.
  - Make a walkthrough of your physical building facilities looking for physical or audible information that can be obtained by unauthorized individuals.
- Enable your team.
  - Have a project kickoff with representatives from all affected departments.
  - Make sure the entire organization is aware that the team will need to have candid answers to their business practices and has authority to require their time.
  - Make sure that senior management (those at risk) has the appropriate level of commitment for information they can provide.
  - Make sure senior management will be available to assist in risk analysis once the gap analysis has been completed.
  - Provide the team with contact information for all areas of your organization being evaluated.



### ***Michael Whitcomb, PMP, CISM***

Michael is the founder and President of **Loricca, Inc.** He has 25 years of experience building and supporting secure systems for government and commercial organizations of all sizes. Michael brings the technical knowledge and proven leadership ability for Loricca to provide world class security services. Since founding Loricca, Michael has established the company's presence providing security solutions to some of the country's largest companies.

Prior to Loricca, Michael served in technical leadership positions, leading and implementing solutions for various clients within both the government and commercial sectors including finance, healthcare, retail and federal government. Michael holds a Bachelor of Science in Management of Information Systems from the University of Phoenix in addition to the PMP and CISM professional certifications.

Loricca, Inc. | [www.loricca.com](http://www.loricca.com) | 813.600.3005 | [mwhitcomb@loricca.com](mailto:mwhitcomb@loricca.com)

---