



SECURITY & COMPLIANCE ANALYSIS (CIPP™)

AN INFORMATION RISK MANAGEMENT CONSULTING FIRM

OUR EXPERTISE:

INFORMATION RISK MANAGEMENT

COMPLIANCE AND CERTIFICATION

SECURITY AWARENESS TRAINING

INFORMATION FORENSICS

WWW.T3I.COM

CAN YOU...

- Provide your **clients and vendors** with acceptable documentation that their information is protected?
- Demonstrate due diligence for information security and privacy in the event of a **breach or audit**?

DO YOU...

- Understand **all** the Federal or State legislation which affect your business?
- Have the appropriate policies & procedures in place to provide controls for monitoring and management?

ARE YOU...

- Confident in your organizations **ability** to demonstrate due diligence for information security and privacy?

TAKE THE INITIAL STEP

In an ongoing effort to ensure the security of our information assets as well as those of our clients, T3i has developed a high level security review called the **CIPP** (Compliance, Infrastructure, Policy and Physical).

CIPP provides our clients with insight into the major issues surrounding the management and maintenance of information and network systems, as mandated by current federal and state regulations.

At the completion of the **CIPP** review, T3i will conduct an executive review and provide a **written** report with findings and recommendations.



Credible Focused Effective

To Schedule Your CIPP Analysis Contact:

T3i

Mark Reedy—Dir. of Sales
 Phone: 678-845-0209 x-201
 E-mail: mreedy@t3i.com

Corporate Offices:

5400 Laurel Springs Pkwy
 Suite 800
 Suwanee, Georgia 30024
 Fax: 678-845-0217

CIPP ELEMENTS	
Compliance	Definition and documentation of company specific requirements for meeting and maintaining compliance, based on business interviews and regulatory research.
Infrastructure and Systems	Overview of the available client documentation and strategic testing of key security elements within the infrastructure
Policy and Process	Review and evaluation of the documented and acknowledged information and network security processes and policies, including employee interviews and evaluations
Physical	Review and evaluation of security measures for one designated facility

SARBANES-OXLEY (SOX)

Recognizing the levels of interconnectivity in American business, SOX **demands** that originating companies enforce adequate levels of corporate governance and information security standards across all their trading relationships. These standards include the protection of sensitive information and , guarantees to the existence and effectiveness of controls of financial fraud and breach prevention.

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY

HIPAA provides a standardization and a privacy mechanism for the protection of sensitive patient information across the complete spectrum of service providers, insurance processors, and benefit payment institutions. Failure to comply with these standards may result in **penalties** of up to \$25,000 per year/requirement, \$50,000 for wrongful disclosure or in some cause up to 10 years in jail.

GRAMM-LEACH-BLILEY ACT (GLBA)

As the most recent Financial Institution Legislative Update, GLBA is a thorough and exact bill to address the information and technology security requirements for the **banking and financial** industry. The comprehensive “Safeguards Rule” provides specific ranges of acceptable solutions for security implementation / maintenance, & overall responsibilities of the financial community.

STATE PRIVACY LEGISLATION

Most of the states have or are adopting some type of **privacy and security** legislation. For example Georgia’s SB230 regarding notification of security breaches carries fines up to \$500 per instance and SB 251 regarding database privacy of consumer information would be up to \$100,000. The challenge is laws apply/change depending on which **states** you do business in.

PAYMENT CARD INDUSTRY DATA SECURITY STANDARDS

With the explosion of **identity theft** and breach of confidentiality for sensitive consumer information, the Credit Card Industry has developed security standards for the industry based on 12 major requirements . These vendor requirements extend to anyone who accepts, transmits, or processes card data. Fines may reach up to \$500,000 non-compliant breaches.

ISO 17799 / 27001

The common criteria framework established in the ISO standards identify best practice requirements for information and network security. Major information security regulations are derived from the ISO17799 standards, therefore compliance with and adherence to this framework addresses regulatory compliance with the majority of requirements for the major legislative acts.



ISO 27001
(ISO 17799 / BS7799)



For Information
Contact T3i Sales:

Corporate Offices:
5400 Laurel Springs Pkwy
Suite 803
Suwanee, Georgia 30024

Phone: 678-845-0209 ext-201
Fax: 678-845-0217
E-mail: sales@t3i.com

T3i ADVANTAGE

Credible	T3i is comprised of some of the most talented and certified information security professionals in the industry. Operating from the position of an "independent and vendor neutral" consulting firm enables T3i to service clients without compromising integrity.
Focused	T3i focuses solely on providing consulting expertise designed to safeguard information assets and protect critical technology infrastructure while ensuring regulatory compliance.
Effective	We deliver expertise and an action plan that effectively maps the specific solutions required to address remediation. Resulting in a secure, operationally effective environment that mitigates risk and successfully aligns business and security goals.