T3i

INFORMATION
SECURITY
COMPLIANCE
RISK MANAGEMENT

WWW.T3i.COM

INFORMATION RISK MANAGEMENT

AN INFORMATION RISK MANAGEMENT CONSULTING FIRM

IS YOUR COMPANY'S DATA SECURE?

CAN YOU...

- Provide your **clients and vendors** with acceptable documentation that their information is protected?

DO YOU...

- Understand **all** the Federal or State legislation which affect your business?

ARE YOU...

- Confident in your organizations **ability** to demonstrate due diligence for information security and privacy in the event of a **breach or audit**?

SECURITY AND COMPLIANCE MANAGEMENT

For most organizations, the ability to demonstrate due diligence for information security and privacy are no longer a choice, but either a Federal, state or industry compliance requirement. Meeting these challenges requires the use of an independent 3RD party assessment firm to help answer the question of **"who's watching the watcher?"**

CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL
CISSP®

T3i is a leading information risk management consulting firm that specializes in security, regulatory compliance and industry certifications. Our holistic approach to security and compliance management is based on the ISO17799 framework. The risk management program at T3i is not merely one assessment or roadmap geared towards compliance, but rather entails multiple assessments and development of an ongoing security initiative to follow best practices and address regulatory concerns.

Risk Management

- **Enterprise** Security Posture Assessments (SPA™)
- Vendor /Product Security and Compliance **Validation**
- Enterprise Security **Policy** Evaluation and Development
- Disaster Recovery / Business Continuity **Planning**
- Digital Forensic Investigations and Incident Response Plans

Security

- **Application** Security Assessments
- Network **Penetration** Testing
- Internal and External **Vulnerability** Scanning
- Administrative Security Framework Assessment
- Enterprise Security **Policy** Evaluation and Development

Certification and Education

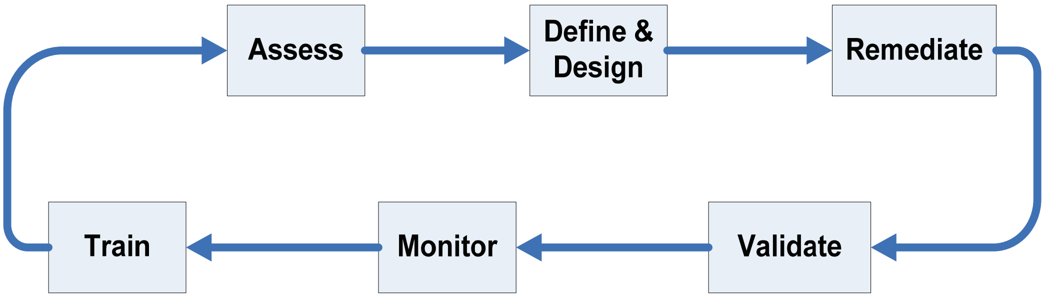
- **ISO 27001/17799** Readiness Evaluation and Remediation
- **PCI / QSA & PA-QSA** Auditing and Compliance
- **SAS 70** Readiness Evaluation and Remediation

Compliance

- **HIPAA , GLBA** and **SOX–404** Compliance Consulting
- Business Process Compliance **Mapping** and GAP **Analysis**
- **Action Plan** Development and **Remediation** Oversight
- Compliance Audit **Support** Services

Defined Methodology

The six (6) step Holistic Security Methodology provides for the continual evaluation and improvement of the security framework. As threats and vulnerabilities, are created by changes in the external world or the business model, this mechanism easily and simply insures continuing security adherence.



Assess
Define & Design
Remediate
Validate
Monitor
Train

PAYMENT CARD INDUSTRY (PCI)SECURITY STANDARDS

WHAT ARE THE PCI SECURITY STANDARDS?

PCI Data Security Standard:

The PCI DSS applies to any entity that stores, processes, and/or transmits cardholder data. It covers technical and operational system components included in or connected to cardholder data. If your business accepts, transmits or processes payment cards, it must comply with the PCI DSS.

PIN Entry Device Security Requirements:

PCI PED applies to manufacturers who specify and implement device characteristics and management for personal identification number (PIN) entry terminals used for payment card financial transactions.

Payment Application Data Security Standard:

The PA-DSS is for software developers and integrators of applications that store, process or transmit payment cardholder data as part of authorization or settlement. It also governs these applications that are sold, distributed or licensed to third parties.

T3I's PCI ENGAGEMENT SPECIFICS

T3i utilizes a standardized methodology to perform compliance validation on all system components where data is processed, stored, or transmitted. This includes all internal or external connections and any data repositories utilized within the transaction process.

T3i is designated by the PCI Security Standard Council as a Qualified Security Assessor Company. The T3i personnel performing the assessment have been trained, tested and certified by the PCI Security Standards Council and are listed on the organizations web site.

PHASE I: Gap Analysis

T3i will provide a comprehensive questionnaire designed to gather all required information (IT, Policy & Procedures, Physical and Company Specific) to assist in the identification of non-compliant areas within the Company's Operations. The Engagement Manager will provide assistance with the completion of the questionnaire. Additionally, the Engagement Manager will be available to address any questions and concerns through the course of the phase.

PHASE II: Gap Analysis Remediation

Upon completion of Phase I, the Engagement team will perform analysis on the information gathered and provide a Gap Analysis Assessment Report. The report will include:

- Overview of the key areas of non compliance
- Identification of existing effective controls
- High level recommendations for remediation
- T3i will provide IT consulting to assist the client achieve a PCI secure topology

PHASE III: Audit & Reporting

A T3i consultant will travel onsite to conduct interviews with key business and operations personnel and perform required tests as outlined in the PCI DSS Security Audit Procedures. Interview questions will be provided prior to the initiation of the onsite audit.

Upon completion of the onsite assessment, T3i will provide "The Company" with the Report of Compliance for submission to the appropriate payment card brand. T3i will submit the Report of Compliance on behalf of the Company, if requested.

In addition, T3i will provide "The Company" with a Compliance Report designed to provide an overview of the protective mechanisms employed by the Company to protect sensitive cardholder data and may serve as a baseline for third party validation.

T3i's Additional PCI Compliance Services

- PCI DSS Policy & Procedure Development
- Internal Vulnerability and Penetration Testing
- Quarterly Network Vulnerability scans by a certified PCI ASV (ControlScan)
- Technical Remediation and Consulting, CISO on Demand

INFORMATION
SECURITY
COMPLIANCE
RISK MANAGEMENT

ISO 27001
(ISO 17799 / BS7799)

For Information

Contact T3i Sales:

sales@t3i.com

Corporate Offices:

3651 Peachtree Pkwy
Suite E-347
Suwanee, Georgia 30024

Phone: 678-845-0209
Fax: 678-297-9611

WHY TAKE PCI SERIOUSLY?

Understanding and implementing the requirements of PCI DSS can seem daunting, especially for merchants without security or a large IT department. However, PCI DSS mostly calls for good, basic security. Even if there was no requirement for PCI compliance, the best practices for security contained in the standard are steps that every business would want to take anyway to protect sensitive data and continuity of operations.

When people say PCI is too hard, many really mean to say compliance is not cheap. The business risks and ultimate costs of non-compliance, however, can vastly exceed implementing PCI DSS; such as fines, legal fees, decreases in stock equity, and especially lost business. Implementing PCI DSS should be part of a sound, basic enterprise security strategy, which requires making this activity part of your ongoing business plan and budget.