



WWW.T3I.COM

INFORMATION SECURITY RISK MANAGEMENT

AN INFORMATION SECURITY RISK MANAGEMENT CONSULTING FIRM

ARE YOUR INFORMATION ASSETS PROTECTED?

OUR EXPERTISE:

INFORMATION
RISK MANAGEMENT

COMPLIANCE AND
CERTIFICATION

INFORMATION
FORENSICS

SECURITY AWARENESS
TRAINING

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?



**Credible & Cost Effective
Information Risk Management**

SECURITY AND COMPLIANCE MANAGEMENT

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.

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. Independent assessments help answer the question of “**who watches the watcher?**”

The ISO program at T3i is not merely one assessment or roadmap geared towards compliance, but rather entails multiple assessments and development of an on-going security initiative to follow best practices and address regulatory concerns.

Service Offerings:

T3i provides "independent and vendor neutral" Consulting services to multiple market segments, including Healthcare, Financial and Technology sectors. The major service offerings include but are not limited to, the following:

- **Independent** Security Posture Assessments
- Vulnerability and **Penetration** Testing
- Vendor /Product Security and Compliance **Validation**
- Visa-**CISSP/PCI** Auditing and Compliance
- **ISO 27001/17799** Readiness Evaluation and Remediation
- **SAS 70** Readiness Evaluation and Remediation
- **Action Plan** Development and **Remediation** Oversight
- Enterprise Security **Policy** Evaluation and Development
- Disaster Recovery / Business Continuity **Planning**
- Security Awareness **Training**
- HIPAA , GLBA and SOX-404 Compliance Consulting

For Information Contact T3i Sales:

Corporate Offices:

5400 Laurel Springs Pkwy
Suite 803
Suwanee, Georgia 30024

Phone: 678-845-0209

Fax: 678-845-0217

E-mail: sales@t3i.com

SECURITY & COMPLIANCE OPTIMIZATION (SCO™)

www.T3i.com

(SCO™) FIVE PHASED APPROACH

PHASE 1 – ASSESSMENT:

Perform a baseline assessment on the existing information systems, network infrastructure, information security policies, procedures, critical business processes and communication systems. The analysis should identify network assets and vulnerabilities as well as the delta between the existing configurations, processes, policies and regulatory requirements, industry standards and best practices.

PHASE 2 – REMEDIATION:

Combine cross compliance mapping with engineering expertise and emerging technologies to design a secure, operationally effective environment that mitigates risk and successfully aligns business and security goals. The solution will leverage existing internal or 3rd party technical resources to identify and address complex and misaligned relationships between individual business processes and information security. Automation and simplification of critical compliance and security processes will be the primary goal in developing a unified information and network security framework.

PHASE 3 – VALIDATE:

Perform regular security audits to validate the effectiveness of the remediation efforts and assist in the enforcement of IT controls, policies and procedures. Validation can occur on an as needed basis or as a part of an ongoing security program, helping to ensure favorable audit results of compliance requirements.

PHASE 4 – EDUCATE:

Provide appropriate educational resources to support and strengthen the security objectives of the organization. The educational initiatives include security awareness training for all users, knowledge transfer for in-house technical staff and awareness of regulatory compliance, process and change management best practices for management.

PHASE 5 – RESPONSE:

Implement a formal Incident/Audit Response program that utilizes security and regulatory expertise to respond, interpret information and provide guidance in the event of an audit, breach or other incident occurs requiring assistance in protecting company assets or reputation.



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

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.

OUR CREDENTIALS

AN INFORMATION SECURITY RISK MANAGEMENT CONSULTING FIRM

	<p>Certified Information Systems Security Professional</p> <p>This CISSP is a vendor-neutral certification governed by the International Information Systems Security Certification Consortium (ISC2). CISSP Certification was designed to recognize competency in the practice of Information Security and is considered one of the premiere security certifications.</p>
	<p>Certified Information Forensics Investigator™</p> <p>This is a designation earned exclusively by the most qualified information forensic professionals in the field. Along with adherence to the highest standards of ethical conduct, the CIFI epitomizes the highest standards in knowledge requirements and expertise. The CIFI encompasses multiple domains of knowledge, practical experience, and a demonstration of expertise and understanding accomplished through a rigorous exam proctored under the most controlled of environments.</p>
	<p>Certified Information Security Manager®</p> <p>The CISM certification is for the individual, who manages, designs, oversees and/or assesses an enterprise's information security (IS). The CISM certification promotes international practices and provides executive management with assurance that those earning the designation have the required experience and knowledge to provide effective security management and consulting services. Individuals earning the CISM certification become part of an elite peer network, attaining a one-of-a-kind credential.</p>
	<p>Certified Internal Systems Auditor</p> <p>The CISA certification insures that client systems are audited and documented based on the current information and AICPA standards for audits. This is a vendor neutral process for evaluating infrastructure, applications, and overall production systems to determine risk and vulnerabilities in the current security environment.</p>
	<p>Cardholder Information Security Program Auditor</p> <p>Based on the PCI standards for information and cardholder security, this certification is awarded to Qualified Data Security Company (QDSC) that has been qualified and meets the strict business and service criteria defined by Visa CISP to perform a PCI Data Security Company Security Assessment according to the PCI Security Audit Procedures.</p>
	<p>HIPAA Certified Security Professional</p> <p>This certification insures that the client information and network security programs are compliant with the 13 documented and accepted security implementation guidelines defined by the US Department of Health and Human Services. An evaluation by a HHS certified vendor insures that client networks meet the defined requirements for compliance.</p>



SECURITY AND COMPLIANCE ANALYSIS (CIPP™)

AN INFORMATION SECURITY RISK MANAGEMENT CONSULTING FIRM

OUR EXPERTISE:

INFORMATION RISK MANAGEMENT

COMPLIANCE AND CERTIFICATION

INFORMATION FORENSICS

SECURITY AWARENESS TRAINING

WWW.T3I.COM

TAKE THE INITIAL STEP

Need: The ever increasing amount of government, industry, and client requirements for proof of standard information and network security programs has created an additional compliance burden for most businesses.

Challenge: Based on the type of client, the type and level of service provided, the geographic location, and the types of connectivity provided, any functional business today will require the ability to demonstrate security competencies.

Solution: 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) Analysis.

The **CIPP™** provides our clients with insight into the major issues surrounding the management, compliance and certification of information and network systems, as mandated by current industry, 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 & Cost Effective Information Risk Management

For Information Contact T3i Sales:

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

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

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



SECURITY POSTURE ASSESSMENT (SPA™)

AN INFORMATION SECURITY RISK MANAGEMENT CONSULTING FIRM

OUR EXPERTISE:

INFORMATION RISK MANAGEMENT

COMPLIANCE AND CERTIFICATION

INFORMATION FORENSICS

SECURITY AWARENESS TRAINING

WWW.T3I.COM



**Credible & Cost Effective
Information Risk Management**

**Please Contact Us To
Schedule Your Assessment**

T3i

Mark Reedy—Dir. of Sales

Phone: 678-845-0209 x201

E-mail: mreedy@t3i.com

Corporate Offices:

5400 Laurel Springs Pkwy

Suite 803

Suwanee, Georgia 30024

ARE YOUR INFORMATION ASSETS PROTECTED?

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. Conducting an independent **Security Posture Assessment (SPA)** is considered to be one of the most effective method of safeguarding information assets and protect critical technology infrastructure while ensuring regulatory compliance.

TAKE THE INITIAL STEP

As an initial step towards strengthening information security, lowering the costs of management, and simplifying the regulatory compliance process, a **Security Posture Assessment (SPA)** will be performed on the information systems, networks, physical security, policy, critical processes, and other areas within the organization.

The purpose of the SPA is multifold:

- To **identify** vulnerabilities within your information security network and perform a **GAP analysis** of the delta between existing configurations, processes, policies and industry best practices
- To provide a detailed **action plan** and recommendations for corrective measures to protect against both internal and external threats
- To serve as a **baseline** assessment in preparation for regulatory audits and for all future information security program initiatives
- To provide a **roadmap** for compliance with regulations including HIPAA, GLBA, VISA-CISP etc.

SERVICE SPECIFICS

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.

T3i's **SPA** will assist management in the development of a unified information and network security framework built around a comprehensive standard. Our clients consider the SPA to be the most effective method of safeguarding information assets and protect critical technology infrastructure while ensuring regulatory compliance.

At the conclusion of the data gathering process, T3i will conduct extensive analysis of the data collected during the assessment to develop a comprehensive security overview and compliance strategy.

Service Includes

While each SPA can be tailored to the specific needs of each client, a typical assessment includes the following:

- Electronic infrastructure mapping
- External frontier scans
- Internal vulnerability scans
- Internal infrastructure configuration
- Network security architecture
- War dialing/modem sweeps
- Wireless security analysis
- Physical security review
- Corporate Information Security Policy review



WWW.T3I.COM

PAYMENT CARD INDUSTRY (PCI) COMPLIANCE

AN INFORMATION SECURITY RISK MANAGEMENT CONSULTING FIRM

OUR EXPERTISE:

INFORMATION RISK MANAGEMENT

COMPLIANCE AND CERTIFICATION

INFORMATION FORENSICS

SECURITY AWARENESS TRAINING

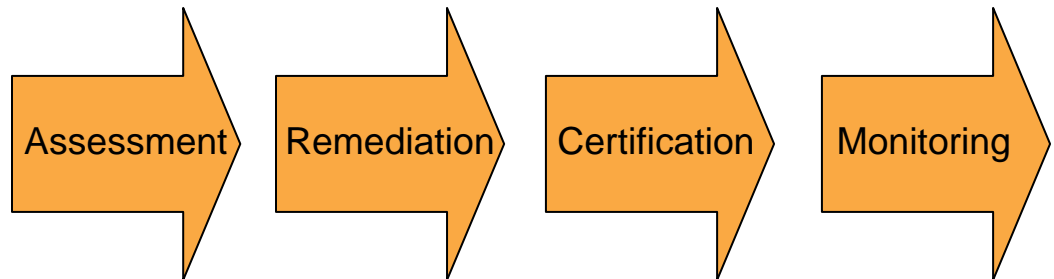
WWW.T3I.COM

Visa's Cardholder Information Security Program (CISP) has been mandated by Visa since June 2001, and is intended to protect Visa cardholder data. To achieve CISP compliance, all members, merchants and service providers must adhere to the Payment Card Industry (PCI) Data Security Standard, which offers a single approach to safeguarding sensitive data for all card brands. Failure to comply can mean revocation of VISA

OUR APPROACH TO VISA CISP CERTIFICATION

CISP compliance validation identifies and corrects vulnerabilities by ensuring appropriate levels of cardholder data security are maintained. As a (QDSC) Qualified Data Security Company, T3i is one of the few security and compliance firms certified by Visa USA, Inc to perform onsite PCI Data Security Assessments.

Our CISP Certification engagement focuses on assessment, remediation, certification and quarterly scans of our client's information and network security. T3i's approach aligns your organizations individual business units with their technology needs according to the PCI Security Audit and Reporting Procedures.



Credible & Cost Effective Information Risk Management

For Information

Contact T3i Sales:

Corporate Offices:

5400 Laurel Springs Pkwy
Suite 803
Suwanee, Georgia 30024

Phone: 678-845-0209

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 for profit.
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.



WWW.T3I.COM

INFORMATION SECURITY AWARENESS TRAINING

AN INFORMATION SECURITY RISK MANAGEMENT CONSULTING FIRM

OUR EXPERTISE:

INFORMATION RISK MANAGEMENT
COMPLIANCE AND CERTIFICATION
INFORMATION FORENSICS
SECURITY AWARENESS TRAINING

WWW.T3I.COM

INFORMATION SECURITY - THE HUMAN ELEMENT

People are often the weakest link in a security chain, often because they are not trained or generally aware of what security is all about. While organizations around the globe routinely employ the use of powerful firewalls, antivirus software and sophisticated intrusion-detection systems to guard precious information assets, they often neglect the most important and vulnerable security component: the human element.

All major regulations that address information security (such as **GLBA**, **HIPAA**, and **FACTA**) require a continuing employee education program and proof of performance. T3i's Security Awareness Training reduces corporate liability and helps ensure regulatory compliance.

We know how difficult it can be for your employees to escape the office for several hours or days of training. That is why we are excited to offer you the convenience of attending our expert training on information security best practices whenever and wherever you want, designed to educate your employees, from board room to break room with an audit trail for each employee.



Credible & Cost Effective
Information Risk Management

PROGRAM SPECIFICS

Courses are available to you and your staff online 24 hours a day, from any location with an Internet connection, in 1 hour modules.

In addition to rich, multimedia virtual classroom training, we include online testing (the results of which can be saved in employees HR files to demonstrate due diligence and regulatory compliance).

We present training in a manner conducive to achieve your security and business goals while focusing on a specific knowledge area as outlined within the industry standards for information security.

If you desire **on-site** training our instructors are all certified information security professionals with credible security certifications such as CISSP, CISM, SSCP, Security+, and others.

[Watch Demo Video](#)

[Visit](#)

www.t3i.com/training



T3i Security Awareness Training Program includes:

- Online training accessible 24x7x365
- Comprehensive training material including presentations and videos
- Perfect for code of compliance
- Self paced modules for flexibility
- Online exams
- Monthly reporting for tracking of student participation and progress
- Optional ability to **customize** course content

For Information

Contact T3i Sales:

Corporate Offices:

5400 Laurel Springs Pkwy
Suite 803
Suwanee, Georgia 30024

Phone: 678-845-0209

Fax: 678-845-0217

E-mail: sales@t3i.com



INFORMATION FORENSICS

AN INFORMATION SECURITY RISK MANAGEMENT CONSULTING FIRM

OUR EXPERTISE:

- INFORMATION RISK MANAGEMENT
- COMPLIANCE AND CERTIFICATION
- INFORMATION FORENSICS
- SECURITY AWARENESS TRAINING

WWW.T3I.COM

PROTECTING INFORMATION ASSETS

As the use of the Internet and computers for business, pleasure and criminal activity increases, the requirement for highly skilled information forensics investigators becomes increasingly more critical.

Electronic evidence gathering (or Information Forensics) can assist in both the prosecution and defense of virtually any civil or criminal case.

Due to the unique nature of the skill set required to properly perform this service, most corporations find that hiring and maintaining qualified and experienced personnel is difficult at best and, more probably, financially impractical for most organizations.

T3i's team of certified information forensics investigators are experts at protecting information assets.



FORENSIC SERVICES

T3i adheres to a strict code of ethics; working closely with law enforcement agencies, legal firms and corporate HR officers we employ the highest industry standards and practices when gathering electronic evidence and conducting information intelligence investigations.

In addition to our client on-site services, T3i has established the **Digital Technology Laboratory** in order to provide client's with an expanded range of hi-tech forensic technology services.



Credible & Cost Effective Information Risk Management

Digital Forensics

- Computer
- Network
- Flash Drives
- Peripherals
- Cell Phones
- IPOD's
- PDA's

Digital Recovery

- Deleted Files
- Deleted Emails
- Passwords
- Graphics

Corporate Investigations:

- Employee Misconduct (HR)
- Corporate Espionage
- Cyber Crime Incidents
- Critical Data Recovery
- On-Call Service Contracts

Legal Counsel Solutions:

- Litigation Support
- Expert Witness Services
- Electronic Evidence Recovery

For Information Contact T3i Sales:

Corporate Offices:
5400 Laurel Springs Pkwy
Bldg. 800, Suite 803
Suwanee, Georgia 30024

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



Certified Information Forensic Investigations