Volpe Information Technology Group, Inc.

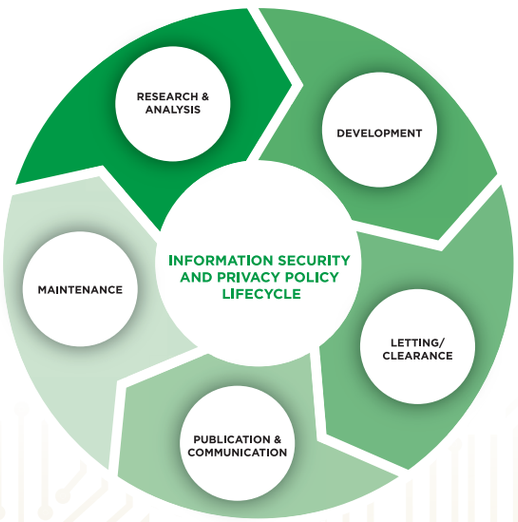
Information Security & Privacy Policy Development

VITG implements a three-tier information security and privacy policy framework consisting of:

- Policy – *establishes organizational wide requirements*
- Standards/guidelines – *provides implementation options and risk based control tailoring and*
- Procedures – *utilizes checklists, templates, and step-by-step instructions to implement controls*

Framework Benefits:

- *Provides easy access to relevant information*
- *Enables customization for a variety of operational environments*
- *Facilitates risk based control tailoring*
- *Achieves cost savings by leveraging control inheritance*
- *Reduces the overhead associated with maintaining and updating policy documents*



VITG Policy Lifecycle

TIER	DRIVERS/INPUTS
1. POLICY Enforceable Maintainable Comprehensive	Laws, Regulations, NIST, OMB, Agency Requirements, etc.
2. STANDARDS/ GUIDELINES Dynamic - changes with Technology	FIPS, NIST 800 Series, New & Emerging Technology, Industry Best Practices
3. PROCEDURES Facilitate the implementation of preventative, detective, and corrective controls	Operational Environment, Physical Location, Common and Hybrid Controls Structure

VITG Policy Framework

VITG leverages a standardized repeatable process designed to work within a defined policy lifecycle. Our process:

- Ensures policies are comprehensive and based upon current laws, regulations, and industry standards
- Engages organizational stakeholders to align policies with business requirements
- Leverages multiple communication strategies to inform organizational stakeholders

POLICY PAST PERFORMANCE:

» *Social Security Administration (SSA)*

» *Centers for Medicare and Medicaid Services*

CONTACT US

Volpe Information Technology Group
bwtech@UMBC North

5520 Research Park Drive, Suite 235
Baltimore, MD 21228

(410) 371-4960
info@volpegroup.com

DUNS: 054243521 System for Awards Management Registered *GSA IT SCHEDULE 70: GS35F535GA*

Volpe Information Technology Group, Inc.

Payment Card Industry (PCI) Advisory Services and Support

PCI Security Standards Council™
PARTICIPATING ORGANIZATION

VITG supports many types of industries to prepare them for PCI Data Security Standards (DSS) audits including financial services, ecommerce, healthcare, and software. We have worked with our customers to provide a structured approach to audit preparation.

Activities include:

- Completion of a Guided Self-Assessment Questionnaire.
- Analyzing and Preparing a targeted report on compliance gaps.
- Proactively providing assessment planning activities and remediation services during the pre-assessment period.
- Adding Integrity, Innovation and Value
  - » *Developing a comprehensive strategy for keeping your company brand, your systems, and your customers safe.*
- Policy and Procedure Development
  - » *Assisting in building a customized set of internal policies to protect sensitive card data to help you meet your PCI compliance requirements.*
- Security Awareness Education.
  - » *Customized training specifically designed to bring those employees responsible for PCI compliance, up to speed.*
  - » *General Security Awareness training including proactive steps to avoid compromise to combat today's dynamic threat environment.*
- Vulnerability Management Services
  - » *Recommend the right tools and services for ongoing vulnerability scanning requirements.*
  - » *Leverage our network of partners to find the right vendor for scanning services.*

PCI PAST PERFORMANCE:

- » *Social Security Administration (SSA)*
- » *Defense Commissary (DECA)*
- » *1st Preference Mortgage Corporation*

We will work with your organization to identify any PCI DSS compliance gaps within your security posture. We can also assist in identifying the scope of your cardholder data environment allowing for creation of a gap analysis remediation action plan prior to compliance validation activities.

VITG'S PCI ADVISORY SERVICES BENEFITS:

- » *Gap Analysis report and assistance. Know where your PCI compliance validation gaps are before you undertake the actual assessment.*
- » *Proactive vs. Reactive approach to compliance validation assessment.*
- » *Identifies and defines your card holder data environment scope prior to PCI assessment.*
- » *Remediation of policy, technical, and other gaps achieving PCI compliance.*
- » *Achieve compliance with PCI documentation requirements.*
- » *Interpret internal and external vulnerability scans and vulnerabilities.*
- » *Educate and make experts of your internal PCI team.*
- » *Prepare your environment for penetration testing.*

CONTACT US

Volpe Information Technology Group
bwtech@UMBC North

5520 Research Park Drive, Suite 235
Baltimore, MD 21228

(410) 371-4960
info@volpegroup.com

DUNS: 054243521 System for Awards Management Registered *GSA IT SCHEDULE 70: GS35F535GA*

Volpe Information Technology Group, Inc.

Software Security Assurance

VITG implements a Software Secure Application Framework for Engineering (SSAFE) which consists of a set of standards, policies and procedures that are tightly integrated into the System Development Life Cycle (SDLC) ensuring that security controls are engineered into the system protecting the confidentiality, integrity, and availability of information.

- SSAFE Framework Benefits:
  - *Encompasses all phases of SDLC from Initiation all the way through Disposal.*
  - *Security always - not just at Security Assessment and Authorization (SA&A) time!*
  - *Address system vulnerabilities throughout the lifecycle.*
  - *Proactive instead of Reactive approach.*

GOAL

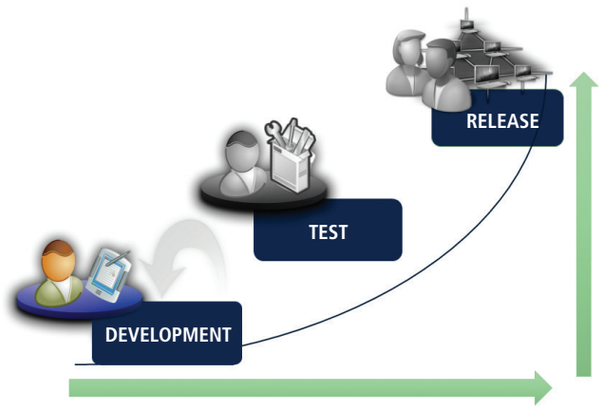
Increase the Quality, Reliability and Security posture of an information system

VITG leverages a standardized repeatable process designed to leverage NIST guidance such as:

- *NIST SP 800-37 - "Guide for Security Authorization of Federal Information Systems - A Security Life Cycle Approach"*
- *NIST SP 800-64 - "Security Considerations in the System Development Life Cycle"*
- *NIST SP 800-53 - "Security and Privacy Controls for Federal Information Systems and Organizations"*
- *NIST SP 800-30 - "Risk Management Guide for Information Technology Systems"*

VITG's SSAFE positions your organization to move to Ongoing Authorization in alignment with NIST and Department of Homeland Security guidelines.

VITG's SSAFE transcends Waterfall and Agile methodologies and works equally well for both.



SOFTWARE SECURITY ASSURANCE PAST PERFORMANCE:

- *Social Security Administration (SSA)*
- *United States Department of Agriculture (USDA)*

NIST PHASE	SDLC PHASE	SAFE ACTIVITY	NIST SP 800-53 CONTROL(S)	OA ACTIVITY
Initiation (Envisioning & Planning)	Requirements Gathering	Business Partner Engagement	SA-1	
		Identify Policies & Standards	SA-1, SA-6	
		Identify Regulatory & Legal Requirements	SA-1, SA-4, SA-7	
		Identify Privacy Requirements	PL-5, SI-7, SI-7(1), SI-7(2), SI-12	YES
		Identify Compliance Requirements	SA-4, SA-8	
		Develop C,I, A* Goals & Objectives	RA-2	YES
		Develop Procurement Requirements	SA-2	
		Perform Risk Assessment	RA-2, RA-3	YES
	Design	Use and Abuse Case Modeling	AC-5, SA-8, SA-11, SC-2	
		Secure Design Review	SA-8	YES
		Secure Architecture Review	SA-8	YES
		Threat & Risk Modeling	RA-2, RA-3	YES
		Generate Security Requirements	SA-4(2), SA-9	YES
		Generate Security Test Cases	SA-11	YES
Acquisition / Development	Development	Writing Secure Code	SA-8, SA-4(1), SA-2(2), SA-10, SI-3(2), SI-10, SI-11, SI-12, SC-2, SC-3 (1), SC-18,	YES
		Security Code Review	SA-11, SI-9, SI-10	YES
		Security Documentation	SA-4(1), (2), SA-5 (1)(2)	YES
	Testing	Security Testing (Fortify 360)	SA-11	YES
		Redo Risk Assessment	RA-2, RA-3	
Implementation / Assessment	Deployment	Secure Installation	SC-7, SC-7(1), SC-7(2), SC-7(3), SC-8, SC-8(1), SC-9, SC-10, SC-15, SC-18, SC-23	YES
		Vulnerability Assessment	SI-2, CA-2, CA-4	YES
		Penetration Testing	SA-11, SI-9	YES
		Security Certification & Accreditation	CA-2	
		Risk Adjustments	RA-2, RA-3	YES
	Maintenance	Change Control	SA-10, CM-3, CM-4,	YES
Operations / Maintenance		Configuration Control (Security Impact Analysis)	CM-1, CM-6, CM-2, CM- 2(1), CM-8, CM-8(1), CM-8(2)	YES
		Recertification & Reaccreditation	CA-2, CA-6, CA-7	
		Incident Handling	IR-1, IR-2, IR-2(1), IR-3, IR-3(1), IR-4, IR-4(1), IR-5, IR-5(1), IR-6, IR-6(1), IR-7, IR-7(1)	YES
		Auditing	AU-2, AU-2(1), AU-2(2), AU- 3, AU-5, AU-7, AU-8	YES
		Continuous Monitoring	CM-4, CM-2(2), CM-1	YES
Disposal	Disposal	Secure Archiving	AU-4, AU-6, AU-6(1), AU- 6(2), AU-9	
		Data Sanitization	AC-15, MP-1, MP-6, MP-6(1), MP-6(2)	
		Secure Disposal	MP-1, MP-4, MP-5, MP- 5(1), MP-5(2), MP-5(3), MP-6, MP-6(1), MP-6(2)	

CONTACT US

Volpe Information Technology Group
bwtech@UMBC North

5520 Research Park Drive, Suite 235
Baltimore, MD 21228

(410) 371-4960
info@volpegroup.com

DUNS: 054243521 System for Awards Management Registered *GSA IT SCHEDULE 70: GS35F535GA*

Volpe Information Technology Group, Inc.

Information Security & Privacy Program Development & Support

VITG implements a traditional Governance, Risk, and Compliance model to ensure alignment of information security and privacy strategies with business objectives.

- Governance – *We leverage a three-tier framework to establish security and privacy policies, standards, and procedures.*
- Risk – *VITG implements a tailored approach based upon the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) and has established differentiators for each of the six steps of the RMF.*
- Compliance – *We implement a continuous assessment methodology aligned with the Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) program to ensure compliance with information security and privacy requirements by focusing on the testing of capabilities.*

TIER	DRIVERS/INPUTS
1. POLICY Enforceable Maintainable Comprehensive	Laws, Regulations, NIST, OMB, Agency Requirements, etc.
2. STANDARDS/ GUIDELINES Dynamic - changes with Technology	FIPS, NIST 800 Series, New & Emerging Technology, Industry Best Practices
3. PROCEDURES Facilitate the implementation of preventative, detective, and corrective controls	Operational Environment, Physical Location, Common and Hybrid Controls Structure

VITG DIFFERENTIATORS

1. **Conduct an enterprise analysis to:**
   - Document a data reference model streamlining the categorization process
   - Integrate automated tools for hardware/ software management to assist with system boundary definition
2. **Develop common control catalogues to assist with control selection and reduce compliance cost.**
3. **Implement automated tools to satisfy control requirements.**
4. **Leverage automated tools to streamline the assessment process.**
5. **Develop risk profiles to support making informed authorized decisions.**
6. **Leverage CDM capabilities, cyber threat intelligence, and assessment results to improve the continuous monitoring program and reduce risk.**

CONTACT US

Volpe Information Technology Group
bwtech@UMBC North

5520 Research Park Drive, Suite 235
Baltimore, MD 21228

(410) 371-4960
info@volpegroup.com

DUNS: 054243521 System for Awards Management Registered *GSA IT SCHEDULE 70: GS35F535GA*