AGENCY CYBER GUIDE 2.0

Agents Council for Technology
Agency Cyber Guide 2.0

Tools for Compliance and Protection in
today's world of Data Breach
and Cybercrime

September, 2018

act™
AGENTS COUNCIL FOR TECHNOLOGY

TABLE OF CONTENTS

> “To competently perform rectifying security service, two critical incident response elements are necessary: information and organization.”
>
> – Robert E. Davis

Compliance and Protection Roadmap:

Handling sensitive information is now one of the most critical responsibilities faced by the modern insurance agency.

Independent insurance agents and brokers must properly collect and protect sensitive client information every day. This means complying with state and federal regulations as well as adhering to customer service best practice standards.

Every state now has data breach response laws, and in the future each state's regulations may vary based on their insurance department's interpretations. The Gramm-Leach-Bliley Act ('GLBA') covers all other models and state laws, including the New York Department of Financial Services (NY DFS) and the new National Association of Insurance Commissioners (NAIC) Model, **which several states have already adopted, and many others are reviewing.**

These acts and regulations can be difficult to address given the multifaceted responsibilities agents encounter daily, but it must be a priority.

The Agents Council for Technology (ACT) in cooperation with our carrier, vendor, and has created this Agency Cyber Guide for Big "I" independent agents and brokers. This tool includes a list of the major Federal and State regulations with clear descriptions and resources to address each, including detailed information on each vendor/service provider. Given the swift nature of change in technology and the increasing sophistication of cybercrime, this tool will be updated on a periodic basis.

12 Steps for a More Secure Agency

1. **Risk Assessment**
2. **Written Security Policy**
3. **Incident Response Plan**
4. **Staff Training and Monitoring**
5. **Penetration Testing/ Vulnerability Assessment**
6. **Access control Protocol**
7. **Written Security Policy for 3rd-Party Service Providers**
8. **Encryption on Non-Public Information**
9. **Designation of CIO**
10. **Audit Trail**
11. **Implementing Multi-Factor Authentication**
12. **Procedure for Disposal of Non-Public Information**

Regulations, Descriptions, Resources

- Note that all regulations listed are critical to comply with GLBA, which also covers other emerging regulation such as NY DFS. These are considered "best practices" for agency security.
- Agencies doing business in the state of New York may apply for an exemption under the NY DFS 23 CRR 500 Act for some of the regulations. However, GLBA still applies. Details on NY DFS exemption eligibility and application are in the 'Appendix' section at the end of this document.

The Gramm-Leach-Bliley Act at a Glance

1. Access controls on customer information systems, including controls to authenticate and permit access only to authorized individuals and systems to prevent employees from providing customer information to unauthorized individuals who seek it through fraudulent means;
2. Access restrictions at physical locations containing customer information;
3. Encryption of electronic customer information, including when in transit or in storage on systems where unauthorized individuals may have access;
4. Procedures to ensure that customer information system modifications are consistent with an organization's information security program;
5. Dual control procedures, segregation of duties and employee background checks for employees with access to customer information;
6. Monitoring of systems and procedures to detect actual and attempted attacks on or intrusion into customer information systems;
7. Response programs for when an organization suspects or detects that unauthorized individuals have gained access to customer information systems;
8. Measures to protect customer information from destruction, loss or damage by environmental hazards or technological failure;
9. Training for staff to implement the security program; and
10. Regular testing of the key controls, systems and procedures of the security program.

Data breaches of large commerce businesses are in the news every day. Small and small to medium-sized agencies **are not immune**. The results can be disastrous. Communicating to your entire client base that your system—which contains their sensitive personal data—has been lost to hackers or cybercrime, can cripple your agency.

It is critial that agents and brokers:

1. understand cyber security requirements
2. begin to comply and protect date
3. follow the road map to fully address all areas that apply to them

Costs and Penalties for Noncompliance:

Non-compliance with any of these regulations may come with a substantial penalty—these can vary by state, as do the data breach communication requirements. Penalties can be assessed as:

- Civil penalties per resident affected and/or per breach;
- Additional penalties for actual economic damages;
- Also punishable by other state-specific deceptive trade practices laws, or as prescribed by a state attorney general;
- The law that applies is the jurisdiction of the person whose data was breached; and
- There are also timelines for responses; may carry penalties for delays in notice.

Facts and Stats

- In 2017, 61% of breaches hit smaller businesses, up from 53% in 2016.[1]
- Cyber-attacks cost small businesses between $84,000 and $148,000[2] and can reach $690,000.[3]
- 60% of small businesses go out of business within six months of an attack.[4]

The Bottom Line

*Non-compliance and lack of action can have **profound implications** on businesses.*

Cyber Strategy Roadmap:

The following compliance and protection roadmap designed to help agencies meet regulatory requirements. ACT recognizes that the threat and regulatory environment is changing rapidly, so we have developed a process to update this document as individual regulations—as well as federal and state laws—change.

1. Risk Assessment

A risk assessment is the identification of hazards that could negatively impact an organization's ability to conduct business. These assessments help identify inherent business risks and provide measures, processes and controls to reduce the impact of these risks to business operations. The assessment should include a risk mitigation checklist.

Resources:

- ACT/CIS 'Cyber Hygiene Toolkits' For hardware & software, the ability to Count, Configure, Control, Patch: Click here to access
- StaySafeOnline.org

2. Written Security Policy

A security policy is a document that states in writing how a company plans to protect the company's physical and information technology (IT) assets. It can also be referred to as a 'written information security policy" or "WISP".

The document must detail your agency's operations for security, governance, inventories, controls, continuity and disaster planning and systems monitoring. This includes internal and external mitigation policies.

Primary Resource

- ACT Cybersecurity Policy Template

Resources:

- Information Shield
- FCC – Cyber Security Planning Guide

3. Incident Response Plan

An incident response is an organized approach to addressing and managing the aftermath of a security breach or attack (also known as an incident). The goal is to handle the situation in a way that limits damage and reduces recovery time and costs while complying with federal and state regulations. This includes communication/ notices to state superintendent upon detection of a cybersecurity event and communication to customers, insurers, and third-party service providers.

This is part of an overall written security plan (see item #2 above).

Resources:

- Mintz-Levin 2017Apr Data Breach Guidelines by State
- NCSL Security Breach Notification Laws by State
- Guidance for Incident Response Plans
- NetGen Data Security

4. Staff Training & Monitoring

This is a critical regulation. Even if all other areas are in compliance, one misstep by agency personnel can expose data due to malware, phishing and other incursions. ACT strongly recommends that all businesses—regardless of size—comply with this regulation.

Resources:

- Phishme.com – Phishing simulator for agency training
- KnowBe4 – Staff security awareness training
- Cybersecurity employee training guidelines from Travelers – Click here
- NetGen Data Security

5. Penetration Testing and Vulnerability Assessment

Penetration testing (also called pen testing) is the annual practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit. This should be done internally and externally.

Vulnerability Assessment is a biannual process that defines, identifies, and classifies the security holes (vulnerabilities) in a computer, network or communications infrastructure.

Resources:

- Tutorials: Differences/Details between Penetration Testing and Vulnerability Assessments
- Veracode - Vulnerability Assessment and Penetration Testing
- Illumant Security Assessment Services - Vulnerability and Penetration testing

6. Access Control Protocol

This responds to regulations requiring restricted access to non-public Information, including PII, PHI, PCI.

Resources:

- FTC.Gov - How to Comply with the 'Privacy of Consumer Financial Information Rule' of the Gramm-Leach-Bliley Act

7. Written Security Policy for Third-Party Service Providers

These are written policies and procedures designed to ensure the security of information systems and nonpublic information that are accessible to, or held by, third-party service providers.

Note: The NAIC refers to this an "information security program."

Resources:

- NetGen Data Security

This is an evolving issue, with regulatory guidance to come.

Note: These elements for the NY DFS regulations do not take effect until Mar 1, 2019. We expect for guidance on this soon and will update this resource.

8. Encryption of Non-Public Information

Encryption is the process of encoding a message so that it can be read only by the sender and the intended recipient.

Non-Public Information refers to all electronic information that is not publicly-available information and for insurance purposes refers to **PII** (personally identifiable information), **PHI** (protected health information), and **PCI** (payment card industry data security standards).

This regulation describes the need to encrypt and protect this data when in storage and when transferred between the insurance agency and its policyholders (email).

Resources:

- What is Data Encryption, How to Get Started
- Comparison of the Best Data Encryption Software - 2017
- ACT – TLS email encryption FAQs
- ACT - Protect Your Clients with Secure Email Using TLS
- ACT – IA Carriers with TLS Secure Email Enabled

Note: There is an exemption to this requirement, however it requires a waiver request to be submitted annually.

9. Designation of Chief Information Officer

This is the title required by NY DFS for some agencies doing business in New York.; nationally this role can be viewed as 'Data Security Coordinator'.

Resources:

- Agency CIO definition and duties (from NY DFS regulation 500.05, page 5)

10. Audit Trail

An audit trail (also called audit log) is an electronic trail that gives a step-by-step documented history of a transaction. It enables an examiner to trace the financial data from general ledger to the source document (invoice, receipt, voucher, etc.). The presence of a reliable and easy to follow audit trail is an indicator of good internal controls instituted by a firm, and forms the basis of objectivity.

For agencies, using your agency management system (with all other interfacing systems) provides a solid foundation for an audit trail.

Resources:

- NIST (Nat'l Institute of Standards & Technology) on Audit Trails

11. Implementing Multi-Factor Authentication

Multifactor authentication (MFA) is a security system that requires more than one method of authentication from different categories of credentials to verify the user's identity for a login or other transaction.

One example is a policyholder logging into an agency website and being requested to enter an additional one-time password (OTP) that the website's authentication server sends to the policyholder's phone or email address.

Resources:

- SBC.com: Protect Your Small Business with Two-Factor Authentication
- CIO.com: Making Multi-Factor Authentication Easy to Use

12. Procedure for Disposal of Non-Public Information

As with encryption, this regulation refers to refers to all electronic information that is not publicly available, including PII, PHI and PCI.

Improper document destruction is often a downfall of small business security.
Regulations on this vary by state. Agents doing business in multiple states should adhere to the highest level of requirements.

Resources:

- Nat'l Conference of State Legislatures (NCSL) - Data Disposal Laws by State

Also, please contact your agency management system provider for their disposal protocol.

Cyber Security Service Providers:

The Agent Council for Technology reviewed the following service providers to understand their ability to help independent agencies comply with the various regulations. Click on the vendor name and find more detailed information on service, rates and contact information.

ACT Cyber Regulation Vendor RFI Process - 2018May

Column1	Regulations	Bear Hill Advisory Group	Cyber Clear Safe	NetGen Data Security	Cyber Vista	Pondurance	RigidBits	RiskSmart	The Mako Group	Vine IT
1	Overall Compliance for Gramm-Leach-Bliley regulations *(individual regulations listed immediately below)*		X			X	X	X	X	X
2	Risk Assessment	X	X	X		X	X	X	X	X
3	Written Security Plan (WISP)		X	X		X	X	X	X	X
4	Incident Response Plan	X	X	X		X	X	X	X	X
5	Staff Training & Monitoring	X	X	X	X	X	X	X	X	X
6	Vulnerability Assessment		X			X	X		X	X
7	Penetration Testing			X		X	X		X	
8	Access Control Protocol	X		X		X	X	X	X	X
9	Written Security Policy for Third-Party Service Providers	X	X	X		X	X	X	X	X
10	Encryption of Non-Public Information					X	X	X		X
11	Chief Information Officer (CIO)		X	X		X			X	X
12	Audit Trail			X		X	X	X	X	X
13	Implementing Multi-Factor Authentication						X			
14	Procedure for Disposal of Non-Public Information			X		X	X		X	X
15	Data Backup						X			X
16	Cyber Liability Insurance			*		*		X		
17	Comprehensive Cybersecurity Assessment			X		X	X	X	X	X
18	***Other***									
	Compromised Credentials on the Dark Web		X				X		X	X
	Continuous Systems Montoring		X			X	X			X
	Cybersecurity Policy		X	X		X	X	X	X	X
	Cybersecurity & Crisis Management Communications Plans	X		X		X	X			
	Executive Cyber Risk Training			X	X		X	X	X	X
	HIPAA Compliance			X		X	X	X		X
	Vendor Risk Management			X		X	X	X	X	

** - Does not sell insurance but has advised clients on how to maximize their cyber liability coverage(s) by implementing a strong information security program.*

Vendor List

Bear Hill Advisory Group

Jack Healey - jhealey@bhagrp.com

www.bhagrp.com

Bear Hill Advisory Group closes 'the gap of grief' that exists between the Board of Directors, Management and IT operations. We develop Cybersecurity Incident Response Plans and the corresponding Cybersecurity Communication Plans for Fortune 100 companies as well as small businesses which clearly articulate the roles and responsibilities of the Board, Management and IT Security. These plans adopt NIST protocols as well as the most current thinking in cybersecurity tactics and strategies. Our plans include a Cyber Escalation Matrix which identifies the impact on an organizations' Information, Operational, Functional, Reputation and Data Recovery in the event of a Cyber Incident.

- **Risk Assessment (Fixed fee based on scope):** Bear Hill Advisory is a business risk identification and mitigation firm. We focus on identifying risks and designing preparedness and resilience plans
- **Incident Response Plan (Fixed fee based on scope):** Jack Healey Bear Hill Advisory are certified in Cybersecurity by the AICPA, SOC for Cybersecurity. Bear Hill Advisory has drafted the incident response plans for companies from 10 million in revenue to 15 billion. We have been drafting plans for over 7 years and use the most up to date tools.
- **Staff Training & Monitoring (Fixed fee based on scope):** Bear Hill Advisory trains senior management and front line response teams on cybersecurity and crisis management.
- **Access Control Protocol (Fixed fee based on scope):** Bear Hill Advisory Access control protocol implements the AICPA SOC TCP protocols.
- **Written Security Policy for Third-Party Service Providers (Fixed fee based on scope):** Bear Hill Advisory are experts in supply chain risk and have designed Cybersecurity as well as supply chain resilience plans. We have been active in the development of plan protocol and monitoring for third parties.
- **Cybersecurity & Crisis Management Communications Plans (Fixed fee based on scope):** We write Cybersecurity and Crisis management Communication Plans, including message maps.

CyberClearSafe

Scott Lindsey - scott@cyberclearsafe.com

Protecting against cyber security threats takes a well thought out plan which addresses all aspects of your organization. Cybersecurity Planning includes: understanding what you need to protect, knowing current safeguards, Threat and Risk analysis, understanding government laws and regulations, preparing an Incident Response Planning, and developing a plan to address gaps in cyber security. CyberClearSafe, founded by Scott Lindsey, is a veteran owned business focused on cyber security, . Scott has over 24 years of insurance brokerage Information Technology experience, as Chief Information Officer (CIO) of a large insurance broker.

- **Overall Compliance for Gramm-Leach-Bliley regulations**
- **(individual regulations listed immediately below) (150):** CyberClearSafe assists organizations understanding GLB and the implications for an Insurance entity. We have extensive experience in interpeting regulatory requirements and technical solutions.
- **Risk Assessment ($500 plus travel at cost):** CyberClearSafe has extensive experience in assessing risk in an organization. We utilize a set of automated tools to assess computer and network systems. We provide detailed reporting on the potential weaknesses and vulnerabilities.
- **Written Information Security Plan (WISP) (150):** We assist in creating a Written Cyber Security Plan for your orangization. This type of project will normally take ongoing dialog and action planning.

- **Incident Response Plan (150):** CyberClearSafe can assist in creating a Cyber Security Incident Response Plan. We will work closely with your organization to build an Incident Response Plans that fits your needs.
- **Staff Training & Monitoring (Varies depending on the number of training videos):** CyberClearSafe has partnered with KnowBe4 to provide Security Awareness training and simulated phishing attacks. We also have the training approved for Continuing Education (in some states).
- **Executive Training (Varies depending on the number of training videos):** CyberClearSafe has partnered with KnowBe4 to provide Security Awareness training and simulated phishing attacks. Training includes modules targeted towards executives. We also have the training approved for Continuing Education (in some states).
- **Vulnerability Assessment (150):** We assist organizations in analyzing weakness and gaps in their security fabric. We are experienced in Vulnerability Assessments and building road maps to improve the organization's security posture.
- **Written Security Policy for Third-Party Service Providers (150):** CyberClearSafe can assist organizations in creating a security policy framework for assessing third-party providers.
- **Chief Information Officer (CIO) (150):** CyberClearSafe can provide strategy and guidance services for agents/brokers. Scott was the CIO for an insurance brokerage for over 20 years. We understand the agent/broker environment and are familiar with the agency management system vendors.
- **Compromised Credentials on the Dark Web (50):** CyberClearSafe provides reporting on compromised credentials on the Dark Web, based on the organization's email domain. We provide an intial report of compromised email addresses and then deliver daily reporting, on newly compromised email addresses.
- **Continuous Systems Montoring (300):** CyberClearSafe provides an appliance (physical or virtual) that will attach to the client's network and look for anomalies based on a user configured rule set. The appliance runs a scan once daily based on the client's desired timeframe. The system will send an email, if any anomolies are detected from over 400 potential issues.
- **Cyber Security Policy (150):** CyberClearSafe will assist an organization in creating or updating their Cyber Security Policy. The Cyber Security Policy is critical in educating employees and setting guidelines for behavior when using the organizations computer and networks.

Cyber Risk Aware (training)

Stephen Burke (Founder) - stephen@cyberriskaware.com

www.cyberriskaware.com

We enable companies to materially reduce cyber risks against their business such as CEO Fraud, Ransomware and data breaches as a result of human error or negligence. We provide continous staff education and awareness content (Mock Phishing, CBT courses, Security Tips and Policy reminders) and assessment methods either on a schedule or immediately in response to detected risky user behaviour by existing defenses. All of our content across 24 security topics is designed using the latest EdTech learning science methods and is brief, enjoyable, and highly engaging.

CyberScout

Eric Hodge - ehodge@cyberscout.com

www.cyberscout.com

Since 2003, CyberScout has been leading the charge against hackers, thieves and even simple human error. We provide unrivaled solutions that deliver valuable prevention education, proactive protection services and swift and appropriate incident remediation for more than 17.5 million households and more than 770,000 businesses.

Our services are provided through more than 660 client partners that include 16 of the top 20 U.S. property and casualty insurance carriers, six of the top seven Canadian insurers, major credit unions, banks and numerous Fortune 500 companies.

Cybertrust

Joe Lagos - jose.lagos@cybertrust.cl

Cybertrust is a company focused on cybersecurity consultancy services, from the strategy of cybersecurity to Cyberforensic investigation, which implies definition of security frameworks, execution of ethical hacking and pen testing services, Security Operation Center and SIEM services, vulnerability management, data privacy and cybercrisis management.

CyberVista

Amjed Saffarini (CEO), Lynn Koreman (info) Lynne.koreman@cybervista.net

CyberVista is a cybersecurity training and workforce development company. Our mission is to create a cyber ready workforce through personalized training programs providing organizations with the people, knowledge and skills required to defend critical assets. In addition to cyber practioner training, we offer board and executive cyber risk training - both in person and on-demand.

- **Staff Training & Monitoring (Pricing differs based on requested offering; enterprise discounts are available.):**
  - Cybersecurity awareness training for staff, online program
  - Cybersecurity certfication training for Security+, CISSP, CISM, and CEH certifications, 100% online
  - CyberVista is a cybersecurity training and education company. We benefit from the rich 80+ year history and success of our sister company Kaplan, one of the world's largest and most diverse education providers. Our platforms are built on the same underpinnings of technology and pedagogy that help Kaplan educate doctors, lawyers, finance, and technology professionals. Additionally, with we partner with the organizations behind the most in-demand cybersecurity certifications such as ISC2, ISACA, and CompTIA. Our certification training programs are official and approved.
- **Executive Training (Custom):** Cybersecurity board and executive training including seminars and table top exercises to help leaders understand cybersecurity as an enterprise risk.

Digital Defense

Meg Grant - Meg.Grant@digitaldefense.com

www.digitaldefense.com

As a global provider of managed and self-managed security risk assessment solutions, Digital Defense's most popular offerings, vulnerability management and penetration testing, are based on our proprietary service delivery platform called Frontline Vulnerability Manager™ . Leveraging our patented technology, Frontline provides a unique underpinning to our solutions that produce higher quality security assessment results for our clients.

The Mako Group (MakoPro)

David Lefever dlefever@makopro.com

www.makopro.com

The Mako Group is a cyber-focused company with risk management, maturity assessments, technical testing services and compliance audit at the core of our business. Founded by an insurance executive, we meet the needs of clients with a knowledge base, process and strategy that has been optimized to face the challenges of the industry. With propriety methods of evaluating organization's cybersecurity posture, we traverse the boundaries between compliance and internally-driven maturity seamlessly to tackle our clients' most pressing challenges. More broadly, our experience within the insurance industry and greater financial services realm gives us comprehensive insight into the challenges of organizations small and large, simple and complex. In

short, we strive for partnerships with clients to form lasting relationships rather than discrete engagements to ensure compliance and maturity goals are realized.

- **Overall Compliance for Gramm-Leach-Bliley regulations (individual regulations listed immediately below) (7500):** The Mako Group started in the banking and financial compliance world and has since develop a robust practice around providing ITGC audits, GLBA compliance checks and meeting shifting regulations at the Federal and state level of banks, insurers and other financial institutions.
- **Risk Assessment (7500):** The Mako Group has a team of experience risk and audit professional who are collectively capable of performing risk assessments against a dozen different frameworks or constructing a custom risk assessment methodology based on individual needs.
- **Written Information Security Plan (WISP) (5000):** A security plan provides the corner stone of any organizations security program. The Mako Group works with each and every one of our clients to develop and improve their written security plan either through recommendations within technical testing reports or direct interaction within risk management engagements.
- **Incident Response Plan (7500):** Every organization has cybersecurity incidents, it is simply a matter of whether the organization is prepared to respond that dictates the impact. The Mako Group has worked with global and local companies alike to develop and implement true incident response plans.
- **Executive Training (3000):** The Mako Group's staff has worked with businesses large and small to implement monitoring programs in the form of email phishing, pre-text calling and physical access reviews. This, coupled with training sessions we offer alongside the engagements, offer superior value to improve the client's staff-based cybersecurity protections.
- **Vulnerability Assessment (3250):** The Mako Group's cybersecurity team has a rich history of providing vulnerability assessment services to a variety of clients that must meet Federal and state compliance objectives. Over 60% of all the assessments performed by The Mako Group are assessing clients with financial compliance objectives.
- **Penetration Testing (4000):** The Mako Group's cybersecurity team has spent years focused on learning the ins and outs of information systems subject to financial compliance requirements. Over 60% of all the assessments performed by The Mako Group are assessing clients with financial compliance objectives.
- **Access Control Protocol (7500):** Controls offer a mechanism for organizations to exert just that: control. The Mako Group works with financial organizations regularly to develop, define, refine, test and evaluate access controls to ensure secure and compliant operations.
- **Written Security Policy for Third-Party Service Providers (3000):** The Mako Group's risk management team works to assess, evaluate, quantify and manage third-party risk management. Throughout that various engagements conducted, third-party service provider security plans are regularly reviewed, amended and/or written.
- **Chief Information Officer (CIO) (2500):** The Mako Group has provided sourced staff in a variety of different roles. Most notably, The Mako Group provided a sourced Chief Information Security Officer (CISO) for a Fortune 500 company.
- **Audit Trail (1500):** The Mako Group has extensive experiencing building, designing and following audit trails within a variety of different environments and for different reasons. Depending on the scope of this process, it can be a single day consulting project or an extensive review of organizational processes.
- **Procedure for Disposal of Non-Public Information (500):** As part of any strong security program, there must be a mechanism for the destruction and disposal of data. This process can be nuanced but is essential for compliance which is why The Mako Group makes a habit out of reviewing this within every ITGC, GLBA, risk or audit engagement.
- **Comprehensive Cybersecurity Assessment (Small: $15,000 Medium: $30,000):** The Mako Group regularly partners with organizations to not just meet compliance goals but assist in on-going maturity efforts, as well. The first stage in this process is a comprehensive cybersecurity assessment that looks at technical, management, risk and audit programs within an organization as they relate to cybersecurity and compliance. This process includes the bulk of the elements discussed in 1 through16 but dramatically reduces the overall cost by preventing management, reporting, discovery and assessment activities from being needlessly repeated. The Mako Group bases pricing for this primarily off size with some interest in maturity.
- **Compromised Credentials on the Dark Web (Included within a variety of services or standalone based on number of users):** The Mako Group utilizes a variety of different reconnaissance and OSINT techniques to search for compromised credentials on the dark web. This process is generally included within other services offered but can be offered as a standalone service.

- **Cyber Security Policy ($2000 - $5000):** The Mako Group has a long history of partnership with clients on their road toward compliance and cybersecurity maturity. We often evaluate cybersecurity policies for more than compliance but for the opportunity for expansion, maturing and growth over time.
- **HIPAA Compliance (Small: $7,500, Medium: $15,000):** One of The Mako Group's core service offerings is HIPAA risk assessments and audits. Our experience ranges from single office organizations to multi-state networks with mature HIPAA environments.
- **Vendor Risk Management (Small: $7,500, Medium: $15,000):** The Mako Group offers a variety of vendor risk management services and the exact scope depends on the needs of individual organizations. In general, we perform reviews of vendor risk management processes or cybersecurity review of vendors depending on the goals of the organization.

NetGen Data Security

Judi Newman - judi@netgendatasecurity.com, bill@netgendatasecurity.com

www.netgendatasecurity.com

NetGen is a combination of Phaze II Consulting and ProfitProtection Risk Management both independent consulting firms working within the insurance agency arena. As hacking activities increased we saw that insurance agencies needed a product that would enable them to realistically move towards compliance with GLBA.

- **Risk Assessment:** Compliance Toolkit and consulting services $250 plus. Dependent on program best suited to agency based on size, etc. NetGen has over a combined 50 years of working with insurance agencies in a multitude of areas of management. The requirements of HIPAA/HITECH in 2003 was the beginning of assisting agencies in moving towards the GLBA compliance requirements.

Pondurance

Ron Pelletier (CEO), Mike Childs - info@pondurance.com, mike.childs@pondurance.com

www.pondurance.com

Pondurance has a wide range of experience working with insurance companies over the past ten years but little with Independent Agents. The experience with insurance companies includes risk assessments, penetration testing, application security testing, social engineering, policy & plan development, security awareness training and many others.

- **Overall Compliance for Gramm-Leach-Bliley regulations (individual regulations listed immediately below) ($150.00 - $306.00):** Pondurance has a wide range of experience working with insurance companies over the past ten years but little with Independent Agents. The experience with insurance companies includes risk assessments, penetration testing, application security testing, social engineering, policy & plan development, security awareness training and many others.
- **Risk Assessment ($150.00 - $306.00):** Our team of information security consultants has many years of experience with helping clients to assess their current information security posture and to develop remediation and risk reduction plans. This Life-Cycle Driven approach fosters a secure IT and information environment, and it helps our clients harmonize their compliance efforts related to regulatory mandates, industry standards, and frameworks such as FFIEC, PCI DSS, HIPAA, NERC-CIP, GLBA, COBIT, ISO 27001/2, and others. Our knowledge of industry trends and cutting edge technical vulnerabilities provide our clients with a formidable, yet cost-effective, ally in information security.
- **Written Information Security Plan (WISP) ($150.00 - $306.00):** Ponduarnce has worked with more than 100 organizations to develop and document Information Security Plans/Programs based upon several standard frameworks.

- **Incident Response Plan ($150.00 - $306.00):** Pondurance develops a Cybersecurity Incident Response Plan (CIRP) customized to each client's environment. Our methodology is consistent with National Institute of Standards and Technology (NIST) recommendations across the incident handling lifecycle; Prepare, Identify, Contain, Eradicate, Recover, Learn.
- **Staff Training & Monitoring (Per user pricing baased on number of users and level of training):** Pondurance has partnered with KnowBe4 to offer security awareness training and on-going effectiveness testing of that training. We also help clients develop training and awareness policies and procedures.
- **Vulnerability Assessment ($150.00 - $306.00):** Pondurance approaches Vulnerability Assessment exactly like we do Penetration Testing (see below) without the final step of Controlled Penetration Testing. The same documentation is delivered.
- **Penetration Testing ($150.00 - $306.00):** Pondurance has performed hundreds of penetration tests. We have developed a methodology that is exacting yet flexible to meet our clients' needs. The methodology includes the following steps: Information Gathering, Vulnerability Discovery, Verification & Manual Testing, Controlled Penetration Testing. We also develop and deliver a full set of documentation detailing the scope of the scope of the testing, the findings and suggested remediation steps to eliminate discovered vulnerabilities. This approach meets the requirements for penetration testing of all compliance standards.
- **Access Control Protocol ($150.00 - $306.00)**: Pondurance provides consulting and developing of policies and procedures for access control protocols
- **Written Security Policy for Third-Party Service Providers ($150.00 - $306.00):** Pondurance provides consulting and developing of policies and procedures for security policies
- **Encryption of Non-Public Information ($150.00 - $306.00):** Pondurance provides consulting and developing of policies and procedures for encryption
- **Chief Information Officer (CIO) ($150.00 - $306.00):** Pondurance has successfully served organizations of varying sizes as a Virtual Information Security Officer and other similar co-sourcing partnerships within highly regulated industries such as healthcare, utilities and finance. Our success in these partnerships is attributable to our team of more than 50 professionals, the majority of whom are in client service roles. The depth and breadth of experience within our team allows the Virtual Information Security Officer to position the right team member to fill our client needs at the right time. While our Virtual Information Security Officers typically are available during standard business hours, Pondurance's 24/7 Security Operations Center and Security Incident Hotline allow us to respond to clients in minutes by phone, live chat and email 365 days a year in the event of a security incident or breach.
    - Further, Pondurance's flexibility of approach allows us to address the needs of our clients of varying sizes and requirements through scaling the extent and timing of our involvement. Pondurance has engaged in such partnership arrangements for many years and has multiple ongoing projects in this service line.
- **Audit Trail (Custom):** Pondurance's Threat Hunting + Response services include logging of security events and storage of those logs to provide an audit trail. The storage capacity is dependent on client needs and regulatory requirements.
- **Procedure for Disposal of Non-Public Information ($150.00 - $306.00):** Pondurance provides consulting and developing of policies and procedures for Disposal of Non-Public Information
- **Cyber Liability Insurance ($150.00 - $306.00):** * Pondurance does not sell insurance but has advised clients on how to maximize their cyber liability coverage(s) by implementing a strong information security program.

Rigid Bits - HIPAA Compliant

Ryan Smith - ryan@rigidbits.com

www.rigidbits.com

- ISSA member
- Certified Information Systems Security Professional (CISSP)
- Certified Penetration Tester (GPEN)
- Offensive Security Wireless Professional (OSWP)
- GIAC Certified Forensic Analyst (GCFA)
- EnCase Certified Examiner (EnC)

Rigid Bits provides affordable proactive and reactive cybersecurity services for businesses of all sizes. Our approach is focussed around building a strong understanding the companies we serve to reduce risk while optimizing operational efficiency and meeting budgetary needs. We work closely with internal or 3rd party IT to help them test and re-enforce the systems that your business depends on. We can tailor an information security program that fits your risk and the specific regulations that apply to your business.

- **Overall Compliance for Gramm-Leach-Bliley regulations (individual regulations listed immediately below) (Starting at $300):** Rigid Bits consultants have experience helping businesses with many different forms of compliance requirements. Agencies can use our expertise to get help as they work to meet the requirements for GLBA, HIPAA, State Laws, PCI, and other regulations. Being compliant does not guarantee you are fully secure, so we also will advise on best practices based on NIST standards and from our years of experience.
- **Staff Training & Monitoring (Starting at $58):** Rigid Bits has partnered with KnowBe4, a premier security awareness training and testing company. As a partner, we have access to training modules, phishing campaigns, and analytics tracking to show company progress.
- **Executive Training (Starting at $58):** Rigid Bits has partnered with KnowBe4, a premier security awareness training and testing company. As a partner, we have access to training modules, phishing campaigns, and analytics tracking to show company progress.
- **Vulnerability Assessment (150):** Vulnerability assessments through Rigid Bits provides you with an in-depth view of your systems' security level. Assessments are done by an experienced analyst to ensure reports include more than just a list of vulnerabilities but also include an executive summary to help you understand what these risks mean. Our results are reviewed with clients to identify vulnerabilities that are most significant as well as remediation recommendations to ensure the clients' risks can be addressed.
- **Penetration Testing (Starting at $3,600):** Rigid Bits analysts have extensive experience performing Penetration Tests and are all certified from GIAC. Testing begins with a Vulnerability Assessment. We then use real-world attacks to exploit systems and gain access to sensitive information. At the end of the test, we provide details about real world attack scenarios and show the risk to sensitive company data and resources. Our detailed report serves to educate executives while providing sufficient detail for technical/IT staff.
- **Access Control Protocol (Included with Risk Assessment and Policies & Procedures Review):** Rigid Bits consultants assist with policies and procedures development that aligns with NIST standards, including your access control protocol.
- **Encryption of Non-Public Information (Included with Risk Assessment and Policies & Procedures Review):** Rigid Bits consultants assist with policies and procedures development that aligns with NIST standards, including the policy for encryption of non-public information.
- **Audit Trail (Included with Risk Assessment and Policies & Procedures Review):** Rigid Bits consultants assist with policies and procedures development that aligns with NIST standards, including the policy for documentation and audit trails.
- **Procedure for Disposal of Non-Public Information (Included with Risk Assessment and Policies & Procedures Review):** Rigid Bits consultants assist with policies and procedures development that aligns with NIST standards, including the policy for disposal of non-public information.
- **Comprehensive Cybersecurity Assessment (250):** Rigid Bits can provide a Comprehensive Cybersecurity Assessment as part of other offerings and packages. Our apporach drives understanding and knowledge around risks and security awareness.
- **Compromised Credentials on the Dark Web (Starting at $75 Included with some packages):** Rigid Bits has access to Dark Web monitoring services to help clients know when their credentials have been posted for sale by hackers. We can run a free initial scan that goes back 2 years. Additional details are available when subscribing to the full service.
- **Cyber Security Policy (Included with Risk Assessment and Policies & Procedures Review):** Rigid Bits will advise on updates to your Cybersecurity Policy and Information Security Program as part of your overarching Policies & Procedures.
- **Security Snapshot (499):** Rigid Bits offers a security snapshot to businesses that want to gain more knowledge of their systems and network activity or for those that are suspicious of a breach but not ready to invest in a formal investigation. Our process a utilizes a network data capture and expert analysis to give you a better understanding of your system and network activity. With this type of analysis, we can identify malware, compromises, misconfigurations and other possible threats to your security.

- **Vendor Risk Management (Included with Risk Assessment and Policies & Procedures Review):** Rigid Bits addresses vendor risk management as part of the 3rd party service provider security program requirements that need to be reflected in your Policies & Procedures. Furthermore, when completing a Risk Assessment, we will look closely at risks involved with these types of relationships.
- **Risk Assessment (Starting at $240):** Our Risk Assessment includes a Policies & Procedures Review to align your supporting documents with the risks identified during the assessment. During the process, we guide you through questions that will help us analyze and understand your true risks. Our approach uses CIS Critical Controls as a baseline.
- **Written Information Security Plan (WISP) (250):** Rigid Bits provides an experienced analysts that can provide guidance and support for your agency's information security plan. We begin at a high level with customers that have not yet put controls in place and ensure, at a minimum, the top 6 controls are addressed. We map our controls to the CIS Top 20.
- **Incident Response Plan (Starting at $120):** With a more than a decade of experience with computer forensics, Rigid Bits analysts apply their knowledge and insight to developing your agency's Incident Response Plan. Even with a solid cybersecurity practice in place, how you respond to an incident can greatly impact your ability to quickly contain a breach. Just like a fire drill, it's important to have a plan and test that it works. Rigid Bits experts will work with you to develop a well thought out Incident Response Plan that is based off of experience, NIST best practices, and your specific needs.
- **Written Security Policy for Third-Party Service Providers (Included with Risk Assessment and Policies & Procedures Review):** Rigid Bits consultants assist with policies and procedures development that aligns with NIST standards, including the 3rd party service provider security policy.
- **Continuous Systems Montoring (Starts at $6):** Rigid Bits offers continuous endpoint breach detection to notify us when clients have potentially unwanted or unsafe software on their endpoints, these typically indicate hacker footholds that bypass antivirus and firewalls.
- **Cybersecurity & Crisis Management Communications Plans (Included in Incident Response Plan Development):** Rigid Bits includes Cybersecurity and Crisis Management Communications as part of their Incident Response Plan.
- **HIPAA Compliance (Included with Risk Assessment and Policies & Procedures Review):** Rigid Bits will advise on updates to your Cybersecurity Policy and Information Security Program as part of your overarching Policies & Procedures.

RiskSmart

Terry Schwarting - tschwarting@risksmartadvisors.com

www.risksmartadvisors.com

Our RISKPORTAL is a subscription based cost-effective GRC tool for companies large and small to efficiently address and manage information security and compliance risk. Through our RISKPORTAL, users efficiently analyze up-to-date information as opposed to chasing outdated information. Our comprehensive array of services enables customers and subscribers to systematically record, store, analyze, share and act upon enterprise-wide information security and compliance data. Our RISKTOOLKIT also enables companies to generate reports and summaries of this data and share them with authorized personnel across multiple business groups and extended information sharing networks. Most of the features of our service can be accessed through a variety of devices, including laptop computers, tablets and mobile devices. Furthermore, our RISKTOOLKIT offers training modules and digitized documentation policies for our clients to utilize as part of their risk mitigation plan.

- **Overall Compliance for Gramm-Leach-Bliley regulations (individual regulations listed immediately below):** Have several Mutual Insurance companies as clients, and working with agencies, captive and independent.
- **Risk Assessment ($300-$500):** Full/compact/customized assessments available, custom assessment may require development fee.
- **Written Information Security Plan (WISP) ($200-$260):** Managed services can assist in this process.
- **Incident Response Plan ($500/year):** Included in our WISP (Written Information Security Policy) offering of our RiskToolKit.

- **Staff Training & Monitoring ($15-$25):** LMS system within our RiskToolKit for employee training surrouding information security and compliance
- **Executive Training ($15-$25):** LMS system within our RiskToolKit for employee training surrouding information security and compliance
- **Access Control Protocol ($500/year):** Included in our WISP (Written Information Security Policy) offering of our RiskToolKit.
- **Written Security Policy for Third-Party Service Providers (500):** Enterprise grade WISP documents within our RiskToolKit derived from ISO 27000
- **Encryption of Non-Public Information (None - Part of assessment):** All reports generated through submitted assessments reside in a fully-encypted database
- **Audit Trail (included with assessment):** Full reporting of submitted assessments reside in fully encrypted database within our RiskToolKit
- **Cyber Liability Insurance:** Can provide suggestions within our network of insurance professionals
- **Comprehensive Cybersecurity Assessment ($500/year):** Our RiskPortal is assessment agnostic. We can provide assessment analytics and reports for full assessments of any framework.
- **HIPAA Compliance ($500-$1000/year):** We provide complete and compact assessments for organizations required to comply with HIPAA compliance, as well as include HIPAA policies as part of our WISP documents
- **Vendor Risk Management (estimate per business):** Full product suite of tools for Vendors, Business Partners, Subsidiaries and Branch offices to begin remediating areas of information security and compliance deficiency.

Vine IT Security Services

Nathan Ginter - nginter@vineit.com

www.vineitsecurity.com

In today's advanced digital age you need software and people to ensure the highest level of security. We have blended the best security experts in the industry, the best software available and a team of dedicated support technicians available 24/7 to fundamentally change the way businesses think about IT, Security, Compliance and Support.

- **Overall Compliance for Gramm-Leach-Bliley regulations (individual regulations listed immediately below) ($5,000 Assessment Bundle $5000 Policy and Procedure Bundle):** Vine IT is a veteran owned, SMB focused national managed IT and security consulting firm based in St. Petersburg, Florida. Experienced in performing HIPAA, ALTA Pillar 3, and GLBA assessments. We perform full service risk assessment, policy development, and even offer remediation services as necessary.
- **Risk Assessment (Part of $5,000 Assessment Bundle):** Vine IT performs risk assessments covering all aspects of IT related GLBA, HIPAA, and ALTA Pillar 3 requirements. We used a customized version of the NIST IT framework. Assessments cover administrative, technical, and process control standards and provide both a risk register and remediation recommendations.
- **Written Information Security Plan (WISP) (Part of $5000 Policy and Procedure Development Bundle):** Vine IT offers scratch policy and procedure development based on findings and information gathered during the risk assessment phase of service delivery. Our analysts create a custom package incorporating many elements necessary for compliance as a complete "all-in-one" solution.
- **Incident Response Plan (Part of $5000 Policy and Procedure Development Bundle):** Vine IT offers scratch incident response procedure development based on findings and information gathered during the risk assessment phase of service delivery. For managed services clients, Vine IT offers end to end incident response, remediation, and logging as part of our service portfolio.
- **Staff Training & Monitoring (Varies by user count and chose service package. Employee training implementation is typically $3,000 - $4,000.):** Vine IT offers implementation of the web based cybersecurity training platform Knowbe4. In addition, we offer implementation and support of various employee monitoring softwares for both managed and non-managed clients.
- **Executive Training (Varies by user count and chose service package. Typical price for up to 25 people $3,000 - $4,000.):** Vine IT offers implementation of the web based cybersecurity training platform Knowbe4. This platform includes several tiers including management and oversight level training.

- **Vulnerability Assessment (Part of $5,000 Assessment Bundle):** Vine IT provides comprehensive internal and external vulnerability analysis as part of our assessment bundle. We use the OPENVAS platform which provides details on CVE's found, and ranks them according to risk level and likelihood of success. We also offer remediation of noted vulnerability issues as a separate service.
- **Access Control Protocol (Part of $5,000 Assessment Bundle):** Vine IT performs analysis of in place access controls as part of our risk assessment process. Controls are analyzed in accordance with NIST Cybersecurity framework standards.
- **Written Security Policy for Third-Party Service Providers (Part of $5000 Policy and Procedure Development Bundle):** Vine IT includes 3rd party providers in both the assessment and policy development offerings. In addition we provide templates for business associate agreements / non disclosure agreements as part of our police and procedure development bundle.
- **Encryption of Non-Public Information (Part of $5,000 Assessment Bundle):** Vine IT performs analysis of in encryption controls as part of our risk assessment process. Controls are analyzed in accordance with NIST Cybersecurity framework standards.
- **Chief Information Officer (CIO) (Per-Project Based on Scope):** Vine IT offers a wide scope of network, software, hardware, and cloud presence design and implementation services. Whether a client is looking to move to platforms such as Google Apps / Office 365, or move their infrastructure from their offices to a cloud server system, we can help.
- **Audit Trail (Part of $5,000 Assessment Bundle):** Vine IT performs analysis of auditing, logging, and reporting controls as part of our risk assessment process. Controls are analyzed in accordance with NIST Cybersecurity framework standards.
- **Procedure for Disposal of Non-Public Information (Part of $5000 Policy and Procedure Development Bundle):** Vine IT includes NPI disposal controls in both the assessment and policy development offerings.
- **Data Backup (Part of $5000 Policy and Procedure Development Bundle):** Vine IT includes Data Backup controls in both the assessment and policy development offerings. In addition we offering implementation, monitoring, and reporting of Data Backup systems to monthly managed services clients. We can also help outside clients implement Data Backup systems as a project.
- **Comprehensive Cybersecurity Assessment (Part of $5,000 Assessment Bundle):** Vine IT performs risk assessments covering all aspects of IT related GLBA, HIPAA, and ALTA Pillar 3 requirements. We used a customized version of the NIST IT framework. Assessments cover administrative, technical, and process control standards and provide both a risk register and remediation recommendations. While this service is comprehensive and enough for the SMB market to meet their obligations, physical access snooping / programatic penetration testing is not included.
- **Compromised Credentials on the Dark Web (Included with Security and Awairness training offerings at no cost.):** Vine IT offers dark web monitoring as part of the KnowBe4 platform, it is an included service with security and awairness training.
- **Continuous Systems Montoring (Part of $5000 Policy and Procedure Development Bundle):** Vine IT offers a porfolio of IT services including antivirus monitoring, network and hardware monitoring, data backup monitoring, and we also include monthly change management. In addition our clients have access to a 24/7 support desk for any and all needs.
- **Cyber Security Policy (Part of $5000 Policy and Procedure Development Bundle):** Vine IT offers scratch policy and procedure development based on findings and information gathered during the risk assessment phase of service delivery. Our analysts create a custom package incorporating many elements necessary for compliance as a complete "all-in-one" solution.
- **HIPAA Compliance (Part of $5000 Policy and Procedure Development Bundle)**: Vine IT offers scratch policy and procedure development based on findings and information gathered during the risk assessment phase of service delivery. We can tailor policy development specifically to HIPAA regulation and verbage if requested. Our analysts have written policies and procedure for single doctor practices up to entire hospital systems.

Appendix

Additional details on laws driving regulations listed in the ACT Agency Cyber Guide:

- Gramm-Leach-Bliley Act
- NAIC Cybersecurity Recommendations
- NY DFS 23 NYCRR 500 Regulations

  NOTE: For some of the regulations listed in section 500.19 of the NY DFS regulations, agencies doing business in the state of NY can apply for an exemption. In general, qualifying agencies have fewer than 10 employees, or less than $5,000,000 gross annual revenue in each of the past three fiscal years, or less than $10,000,000 in year-end total assets.

  **However, it is strongly encouraged that agencies review and work to comply with these regulations, as they are strong tents of a solid, effective agency security environment.
- Gramm-Leach-Bliley Privacy Law for Producers

Additional insurance solutions:

- NY Exemption Filing information via IIABNY
- Cybersecurity Vendors and Offerings
- Big "I" Cyber Resources

Following are resources for selling Cyber Security Liability Insurance Policies :

**Do not confuse these with agency security processes detailed in this document prior to this section.

- Big 'I' Markets - Cyber Liability Solutions
- A Buyer's Guide to Cyber Insurance – McGuire/Woods

Acknowledgements

ACT would like to thank the Security Issues work group who provided the input and guidance to make this Cyber Guide a reality, as well as our work group Chairs, Steve Aronson and George Robertson.

Independent Insurance Agents & Brokers of America, Inc.

act™
AGENTS COUNCIL FOR TECHNOLOGY