



Clearing the Regulatory Hurdle: Assessing 2009-2010 Regulatory Exposure and Creating a Remediation Work-plan

IANS' Proposal for

April 13, 2009

Description of Work

Over the coming months in this difficult fiscal environment, the CISO of COMPANY and his team will be required to make some far reaching recommendations to the COMPANY senior leadership.

With the advent of a number of new and updated federal and state acts and industry standards, COMPANY must decide how to comply with these overlapping and often opaque requirements.

Questions that COMPANY must answer include:

1. **What do these regulations REALLY mean?** How should we interpret each one of these regulations and standards? Is the COMPANY's interpretation of the regulation or standard "reasonable"? Is it supported by other similar organizations' interpretations?
2. **How much of our existing framework can we use:** COMPANY has worked hard to create a comprehensive Common Security Framework. How much of the compliance efforts for these new requirements can be subsumed in our existing framework?
3. **Do we really need to spend \$1.5 - \$2.0 M?** With budget dollars tight, what are the minimum steps that COMPANY needs to take to be compliant?
4. **What new technologies actually work?** What new technologies – such as Data Loss Prevention (DLP) products, encryption products, record activity monitoring, file level access auditing and data masking – will be actually required in order to be compliant? What are the best products / services in each one of these technology segments for COMPANY?
5. **How do we get all this done?** How do we move fast enough to meet the 2010 budget cycle and to comply with a regulatory requirements deadline?

The IANS proposal discussed below outlines a consulting engagement that would directly address the questions outlined above.

Scope of Work & Methodology

Please see *Attachment One* for an introduction to the IANS consultant team (with their respective professional biographies) that has been assembled for this project.

The scope and methodology of this consulting project would be the following:

- 1) **Detailed Policy Analysis:** IANS would undertake a detailed analysis of the following information security acts and standards identified by COMPANY as of key interest:

- a. FTC Red Flag Act
- b. HIPAA HITECH Act
- c. Health Care Information Technology Standards Panel (HITSP)
- d. Health Information Trust Alliance (HITRUST)
- e. ISO 27799 – Health Infomatics

Drawing upon the IANS' Research Team, Faculty and extensive Fortune 1000 client base, IANS would present conclusions on what we believe were (or are) the regulators' intentions and what capabilities are required in order for an organization to be deemed "fully compliant" and "minimally compliant".

See *Attachment Two* for a list of respective IANS Faculty Members that would be brought in to support this initiative.

See *Attachment Three* for a diagram of IANS' research clients that would be a valuable benchmarking resource for COMPANY and the IANS consulting team.

- 2) **Initial Fact Finding:** IANS would then conduct in-person and telephone interviews with the COMPANY CISO and key executives / professionals in COMPANY's Information Security, Compliance, Records Management and Risk Management Groups. IANS would also want access to COMPANY's key IT service providers.

The purpose of these interviews would be to:

- a) Understand how COMPANY developed a Common Security Framework to implement a HIPAA compliance strategy. That Common Security Framework is the basis for all major applicable acts and standards within the defined scope.
- b) Identify process and technology solutions COMPANY has put in place in order to address the specific requirements of HIPAA. By knowing how each of the key items in the Common Security Framework is achieved within the company, IANS would better understand the enterprise's current state.
- c) Review 2009-2010 COMPANY's strategic plans for security related improvements. By understanding the firm's near term goals for improving security, IANS could identify any items where COMPANY may not be in current compliance, but clearly has a goal to achieve compliance.
- d) Understand how COMPANY executives are currently planning to meet the compliance requirements for the six current / pending regulations outlined above that may not be in scope of (b).
- e) Understand any specific security or control related objectives that were deferred by COMPANY and the drivers behind those decisions.

- 3) **Interpretation of Acts and Standards:** IANS would consolidate the individual and overlapping regulatory requirements in these acts and standards and develop a comprehensive set of control objectives for COMPANY.

As an industry facing company, IANS has active connections with companies like COMPANY who are facing these same challenges. Using IANS' resources – the Partner Program and our extensive industry contacts – we can provide what other similar organizations are doing to build robust and meaningful control structures – not just a vendor focused or auditor focused view of the control objectives.

IANS can also provide a forward looking view – what these similar organizations believe they must do in the near term and the longer term to build a control structure that not only meets their near term needs, but also aligns with the business to enable growth and reduce risk.

- 4) **Creation of a Custom “Regulatory Heat Map”:** IANS would utilize the Common Security Framework COMPANY has implemented and provide that as an overlay to the Interpretation of Acts and Standards performed in item #3.

Using our understanding of the nature of each control, IANS would then develop a “Regulatory Heat Map” – a table that would quickly and graphically present COMPANY's ability to comply with the most pressing requirements from all six acts and standards outlined above.

See *Figure One* for an illustration of the IANS' consulting end product.

For Illustration Purposes

COMPANY – Regulatory Heat Map

	Organizational Security Policy	Security Governance Structure	Risk Ranking of All Assets	Risk Based protection method of all assets	Known status of all holders of data
FTC Red Flag Act		Does not apply	Applicable only as it applies to data elements and activities that might indicate that actions taken were not properly authorized by the consumer.		Requires evidence that access is granted based on define role with specific removal within 24 hours where access is confirmed not required.
HIPAA HITECH Act					
Health Care Information Technology Standards Panel (HITSP)			Requires full inventory of all data fields	Assumes that business unit owners have been assigned – not just technology owners.	
Health Information Trust Alliance (HITRUST)				Assumes that business unit owners have been assigned – not just technology owners.	Requires a full and detailed chain of custody
ISO 27799					

COMPANY will be able to use the “Heat Map” to identify the areas of most immediate need and clearly articulate how their security strategy is aligned with the regulatory requirements and industry standards. It also will enable COMPANY management to demonstrate that they have a clear vision to not only meet compliance objectives but to identify areas where further change is needed over time to make the controls robust and sustainable.

- 5) **Develop Tactical Work Plan:** IANS would then develop a list of recommended controls – both new and additive to the existing controls – that will allow

COMPANY to develop a plan of attack for any deficiencies in their existing control structure.

IANS would provide the COMPANY team with a combination of technology solutions and process solutions that are tailored to the nature of your business and are mindful of both the near term and long term objectives of your program.

Our industry relationships allow IANS to understand the tools and techniques that have been proven in companies like COMPANY. That direct peer feedback would help COMPANY stress test software/hardware vendor assurances and define not just the “what’s” of compliance but “how” and “why” other companies are making changes to their business process and their technology infrastructure.

- 6) **Periodic Monitoring of COMPANY progress:** Industry acts, standards and regulations are subject to revision and interpretation – especially during the first year that they are in place.

IANS would continue to monitor key changes to the acts and standards and provide periodic updates based on direct feedback from the legislative and governing bodies as well as feedback from our network of research clients.

IANS would use this data to periodically refine not only the Heat Map but also the Tactical Work Plan to ensure that COMPANY’s strategy continues to be adequately scoped and addressing the highest priority areas.

Deliverables

This project would have three specific deliverables:

A) “Regulatory Heat Map” – A color coded grid listing a distillation of the relevant acts and legislations and how COMPANY can meet the spirit of those requirements

B) Tactical Work Plan – A list of recommendations – including People, Process and Technology – that would enable COMPANY to develop a plan to address any identified gaps. Recommendations would be inclusive of improvements that have already been scheduled by COMPANY.

C) Executive Presentation – A simplified version of items A& B distilled to 4-5 PowerPoint slides would be created that explains the nature of the analysis and provides clear recommendations.

Delivery Schedule

We would propose the following target dates and deliverables:

IANS Activity	Activity	Proposed Timing
0) Project Kick-off	A 2 hour face-to-face project kickoff to introduce project objectives, key players, schedule and milestones and logistical data.	1 Day
1) Detailed Policy Analysis & Interpretation	Perform detailed analysis of relevant acts and regulations to identify common elements and outliers.	1 week
2) Initial Fact Finding (Interviews)	Conduct 8-12 interviews of key individuals in COMPANY information security, risk management, records management, compliance and IT organization.	2 weeks
3) Interpretation of Acts and Standards	Interpret both the stated and implied requirements from the six acts and standards.	1 week (concurrent with Step 2 Above)
4) Creation of Regulatory Heat Map	Use results of Steps #1 - #3 to develop Regulatory Heat Map	1 week
5) Develop Tactical Work-plan	Use results from Steps #1 - #4 to develop a detailed tactical work-plan.	2 weeks
6) Periodic Monitoring of COMPANY Progress	Q2, Q3 and Q4 of 2009	To be determined with the client
TOTAL PROPOSED TIMING		6 WEEKS

Of course, these dates are subject to availability and the workload of the key internal COMPANY executives.

Pricing

IANS is committed to minimizing and mitigating the risks associated with project management. To that effect, all IANS' engagements are fixed price and fixed time.

Based on the initial scope defined during discussions with COMPANY and the requirements for this engagement, listed below is the proposed cost of this engagement:

Engagement	Cost	Duration
Clearing the Regulatory Hurdle: Assessing COMPANY's 2009-2010 Regulatory Exposure and Creating a Remediation Work-plan	\$TBD	As defined in the Delivery Schedule section listed above.

Project Cost Assumptions

- IANS would invoice COMPANY for ½ of the total amount of the engagement at the start of engagement with *Due upon Receipt* Payment Terms.
- IANS would invoice COMPANY for the remaining ½ of the total amount of the engagement at the conclusion of the project with *Due upon Receipt* Payment Terms.
- Travel and expenses are not included in this contract price. These expenses will be pre-approved and billed separately.
- IANS reserves the right to separately price activities not defined in this Statement of Work.

ATTACHMENT ONE

About the Consulting Project Team



Phil Gardner
IANS Founder & Managing Partner

Having built IANS' annual practitioner member offering, Phil oversees all practitioner business at the company. Phil began his career in security with seven years with the U.S. Navy as a Strike Fighter Pilot & Ordnance Requirements Officer. After receiving a Masters in Business Administration from Harvard Business School, he joined Goldman, Sachs & Co. in Mergers & Acquisitions and later became an associate with McKinsey & Company in Boston, MA. In 1996, Phil became one of the founders of Provant, Inc., a publicly traded training company serving the Fortune 1000 and Federal Government. He left Provant in 2000 to launch the Institute for Applied Network Security. Phil is a graduate of Harvard Business School and Harvard College; and, he graduated at the top of his class in US Navy Flight School.



Allan Carey
IANS SVP of Research & Product Development

Allan Carey is the Senior Vice President of Research and Product Development at IANS. In this position, he manages IANS Partner Program, including all research and Working Groups, and provides support for IANS' Forums. Prior to IANS, Mr. Carey spent seven years at IDC, a global provider of market intelligence and advisory services for the IT sector. He developed and managed the Security Services practice and provided in-depth analysis, intelligence and consulting on key aspects of the information security and business continuity services markets. In addition, Allan has served as a business analyst in the IPTelecom group at GTE Internetworking, and as a consultant and project manager within the biotech industry. He has spoken at industry conferences in the U.S., Europe, and Latin America and his comments have appeared in the Boston Globe, BusinessWeek, Fortune, InfoWorld, Network World, The Wall Street Journal, Washington Post, and others. Allan holds an MBA in Finance from Bentley College, and a B.S. in Engineering from the University of Massachusetts - Amherst.



Adam Cardinal
IANS Lead Consultant

Adam Cardinal is an independent consultant with 20 years of experience in information security, risk management and IT governance in the financial services industry with large public and privately held companies – most recently as Information Security Officer for Fidelity Investments' Retail Brokerage Division.

Adam has proven leadership experience supervising engagements with federal and state regulatory agencies and external auditors to define and implement robust solutions that allow companies to grow and mature while effectively managing risk. As a project resource Adam provides guidance for medium and large complexity projects to ensure that security and risk impacts are adequately identified and built into documented requirements.

Over the past 10 year Adam has provided oversight of projects requiring compliance with Sarbanes Oxley, HIPAA, Gramm Leach Bliley, FINRA, NASD, OCC, FHLBB, and FFIEC requirements. In addition Adam provides support for vendor management, RFP/RFI solutions, SAS 70 certification, advanced authentication, and systems hardening.

Adam holds a Certified Information Systems Security Professional (CISSP) from ISC2 and a Certified Information Systems Auditor (CISA) from ISACA, as well as a Bachelors of Science degree from Boston University. He is a member of the Financial Services Information Sharing and Analysis Center (FS-ISAC) and of the High Tech Crime Network (HTCN).

ATTACHMENT TWO

IANS Faculty

Listed below are the biographies and specific expertise of the IANS' Faculty that would be pulled in to support the IANS' COMPANY team throughout this project.

Peter Kuper



Industry Experience: Mr. Kuper has been covering the software industry for over a decade. He was the lead software analyst at Morgan Stanley where he wrote a number of industry-defining reports and market-moving stock calls. Previously, he was a director and equity analyst at SG Cowen, where he covered the software sector with a particular focus on security. He has also been an equity analyst and vice president at FAC/Equities and a research analyst at Keefe, Bruyette & Woods.

Expertise: Information security • Content management • Data leakage

Randy V. Sabett



Industry Experience: As co-chair of the Information Security Committee of the Section of Science and Technology of the American Bar Association, Mr. Sabett edited for Information Security: A Legal, Business, and Technical Handbook and The Digital Signature Guidelines. He was also Co-Rapporteur for the PKI Assessment Guidelines and author of several other publications. Admitted to practice before the USPTO, he is a member of the Maryland, Virginia, and D.C. bars. He is also part of the Commission on Cyber Security for the 44th Presidency.

Expertise: Compliance and regulations • Data classification • eDiscovery • PCI compliance • Risk management • IT licensing

Nick Selby



Industry Experience: Mr. Selby has worked as an IT security consultant to small and mid-sized firms subject to regulatory compliance and strict confidentiality, and covered emerging technologies such as open source, wireless, and software piracy when based in Eastern Europe and Europe. He was Editor at Large for Amsterdam-based Tornado Insider/Tornado Investor, and reported for the International Herald Tribune. He is also an avid Linux hacker and a PHP/MySQL enthusiast.

Expertise: Data classification • Data leakage • Information protection

Brandon Dunlap



Industry Experience: Mr. Dunlap has over 13 years of experience managing business technology risk. He was a Senior Project Manager at a large security products company and led the Information Protection Unit of a Fortune 200 energy company. Serving in roles across a variety of highly regulated industries, he has successfully led all aspects of IT security programs: policies and procedures, oversight and controls, strategy, architecture development, and training.

Expertise: Business technology risk • Compliance and regulations • Configuration management • IAM/Authentication • IT security programs • Management of security • Messaging security • Network access control • Patch management • Security awareness • Policy • Vulnerability management