



---

## **An Introduction to the Nagan Research Group (NRG)**

**family of automated, algorithm based  
risk and compliance assessment protocols**

### **Protocol Family Overview**

# Table of Contents

<u>Section</u>	<u>Page</u>
Introduction.....	3
Overview.....	3
The process.....	4
MOSPOCOM.....	5
C-TPAT.....	6
Prismatic®.....	7
HICOM®.....	8
ISO 17799.....	9
SD/SLG.....	10
Sarbox.....	11
Supply Chain Risk Assessment.....	12
Training.....	13
Custom Applications.....	13
Group Reports.....	14
Application and Usage.....	15
Contact Information.....	15

## Introduction

**The Problem:** The growing complexity of regulatory compliance (Sarbanes Oxley, HIPAA, CA Privacy regulations and more) along with risks in the areas of IT, Internet, Operations, plant and security means you, and your organization, face an increasingly growing set of challenges and reporting requirements. All of which not only pose risks but the threat of fines and litigation.

To address these you need to know:

- The vulnerabilities specific to your organization
- What your priorities should be
- How you should allocate resources
- How you can develop a program based on your specific risk profile
- How to address your exposures (fix, replace, mitigate, transfer)
- How accurate your In-house assurances are

In addition you want this information NOW, you want it to be affordable, and you want it to evolve with the situation

**The Solution.** NRG has developed a family of strategic risk and compliance assessment diagnostic tools that delivers strategic assessments and recommended actions with particular issue of concern, in a timely, cost effective fashion. There are currently six products in the family, described later in this document.

Each diagnostic tool:

- Creates a 'profile' that easily identifies major areas of concern
- Provides recommendations to address shortcomings
- Allows alignment of resources and priorities across the entire organization
- Allows comparisons across time and organizational units
- Provides a consistent, repeatable method to track continuing compliance and risk management progress and issues

## Overview

The NRG protocols are supported by proprietary technology which consists of:

- An automated process using questionnaires and our proprietary algorithms to assess risks and measure compliance
- A design that simplifies updating. Content. Making additions, changes, and creating new, or modified, diagnostic tools a straightforward process.

Questions and recommendations are developed by experienced legal and technical professionals

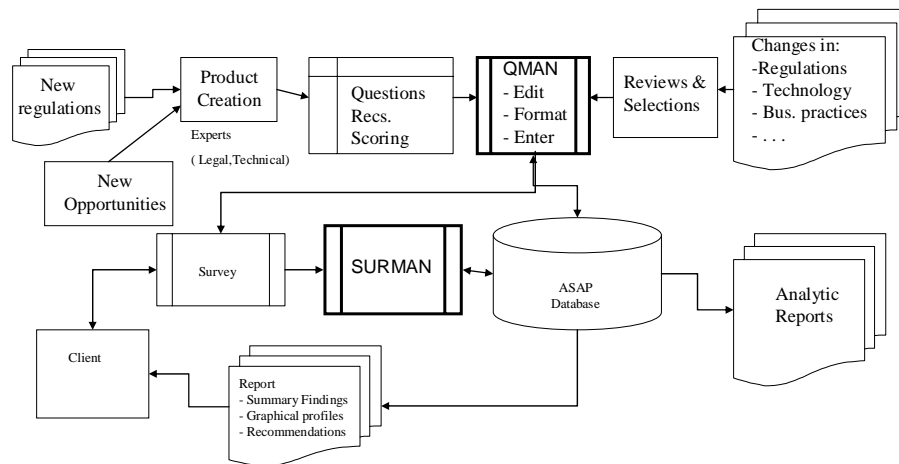
The Protocols:

- Provide clients with a broad strategic overview that evolves with the risk/compliance environment
- Allow alignment of resources and priorities across the entire organization or geography
- Allow comparisons across time and organizational units and geographies
- Does all this in a timely and economic manner

## The process.

- Includes a client questionnaire that is put through a proprietary processing engine creating an overview assessment in major risk areas (depending upon the specific product these may include—legal, technical, regulatory, environmental, business continuity, & disaster recovery)
- Creates a graphical summary with detailed recommendations for each finding (profile)
- Delivers report within two business days of client questionnaire submission
- May result in reduction of insurance costs

### Full Process View



The NRG software platform is the underlying proprietary technology.

The major elements include:

- Our proprietary QMAN software engine that creates and updates the questionnaires in the database.
- QMAN creates, and updates, the products from structured spreadsheet input simplifying new product introduction
- QMAN was designed to allow for ease of updating, additions, change, and the creation of new, or modified, products
- SURMAN processes the client answers, and using the ASAP database automatically creates the output reports.
- Database of questions, responses, scoring data, and recommendations.

# MOSPOCOM

## (Motor Sports Compliance)

Companies in the Motorsports Industry are confronted with a vast array of federal, and state, regulations. A partial list by area follows:

- **Service and Parts Department:** Clean Air act, Clean water act, DOT Hazmat Handling procedures, IRS Inventory Valuation, LIFO/FIFO Accounting, OSHA Regulations, Resource Conservation and Recovery Act, Safe Drinking Water Act, Superfund
- **Consumer Communications:** CAN-SPAM Act, Information Privacy, FTC Internet Usage, FTC Privacy Rule, FTC Prohibition against deceptive and unfair trade practices, FTC Telemarketing sales rule, Required Disclosures, Telephone Consumer protection Act, Truth in Advertising
- **General Management/Personnel:** Age Discrimination in Employment Act, Americans with Disabilities Act, COBRA, Code of Ethics, Employee Drug Testing, Employee Polygraph Protection Act, Equal Pay Act, Family and Medical Leave Act, Federal Child Support Regulations, Federal Wage Hour and Child Labor Laws, HIPAA, Federal Civil Rights Act, Mandatory Workplace Posters,
- **F&I Sales:** Consumer Leasing - Regulation M, Equal Credit Opportunity Act, Fair Credit reporting Act, Fair Debt Collections Practices Act, FTC Credit Practices Rule, Graham Leach Bliley Act, OFAC regulations, Producer Owned Reinsurance Companies, Truth in Lending - Regulation 2, USA Patriot Act (Cash Reporting Rule)
- **Vehicle Sales and Customer Handling:** Credit Card Processing, Deceptive/Unfair Trade Practices, Driver Privacy Protection Act.,, FTC - Door to door rule, FTC - Written warranty rule, IRS treatment of salesperson incentives, LIFO Inventory Accounting Method, Sales to Minors, Spot Deliveries, Straw Purchase

Depending upon their business practice not every dealer will be faced with every regulation. Using an approach of experts, consultants, and legal counsel is just not economically possible, nor is ignoring the possibility of being noticed given the increase in litigation. They need an automated approach that provides:

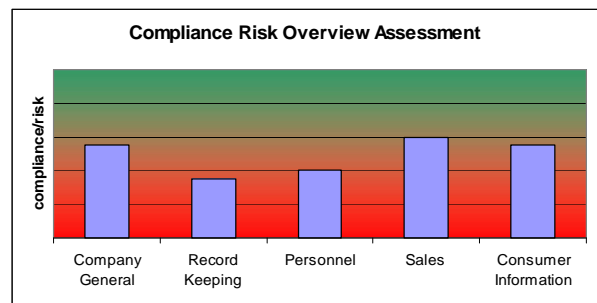
- A strategic overview of their compliance and possible issues
- Information so they can determine priorities and allocate resources rationally
- A way to plan their next steps
- A way to monitor progress on their compliance efforts
- A way to stay abreast of changes in regulations, risks and recommended business practice

They need our MOSPOCOM compliance protocol provided through annual subscription which includes: Three assessments, tracking of progress, and raises awareness of new issues through the MOSPOCOM compliance report.

The compliance report includes a compliance profile, executive summary, graphical summary (example on right) rating rational and recommendations and supplemental material as appropriate.

In addition IRM provide on line quarterly seminars covering the compliance news and observations from experts in the field.

MOSPOCOM provides a way for smaller companies to identify and address their compliance concerns in an economical and timely manner



# C-TPAT

## (Customs Trade Partnership Against Terrorism)

On September 11, 2001, combating the threat of terrorism became US Customs and Border Protection's (CBP) number one priority. 9/11 required CBP to understand that the United States is not immune to terrorist attacks carried out by global terrorists. One of the best means to prevent further terrorist attacks is to use border authorities to make it more difficult for terrorists or terrorist weapons to enter the United States to carry out attacks.

Under CBP's layered, defense-in-depth strategy against terrorism, the Customs and Trade Partnership Against Terrorism (C-TPAT) is the CBP initiative that partners, on a voluntary basis, with members of the trade community. CBP and willing members of the trade community collaborate to better secure the international supply chain to the United States in support of CBP's priority Homeland Security mission.

C-TPAT ASAP – provides importers with a broad assessment of the whole range of supply chain security risks through the use of software, expert databases, and scoring algorithms. C-TPAT ASAP assess business partner requirements, container security, physical access controls, personnel security, procedural security, threat awareness and security training, physical security and information technology security. The basic components of C-TPAT ASAP are a questionnaire, a processing engine, and a database of questions, restatements, and recommendations.

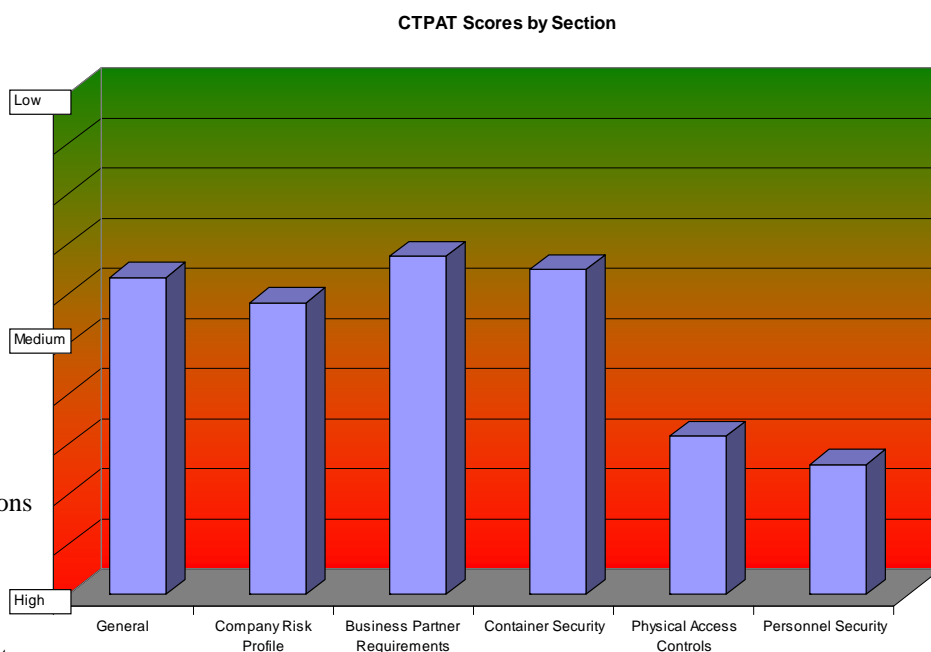
C-TPAT ASAP provides an overview of the broadest possible range of global supply chain risks that an organization faces and collects entity based responses to develop a risk profile. C-TPAT ASAP then generates a road-map of risk, an overview of an organization's supply chain security and concise improvement recommendations for action, in a timely and inexpensive fashion. Companies using C-TPAT ASAP get individual reports by business partners as well as an overall supply chain roll-up and assessment.

The graph summarizes the C-TPAT compliance by the areas in the regulations. The recommendations will provide the basis for an action plan to achieve C-TPAT compliance.

In addition, there is an optional report that can be used as part of the application for C-TPAT compliance once acceptable levels of C-TPAT compliance have been reached.

The service comes in several levels based on number of locations and number of trading partners.

The subscription provides the client, and other members of the supply chain a way to support the annual certification requirement.



# Prismatic®

Prismatic addresses IT, Internet and cyber risks. Currently it assesses over twenty different aspects of risks, ranging from the legal issues in contracts and intellectual property through the myriad technical issues of networks, viruses and data management and protection. The areas currently covered are:

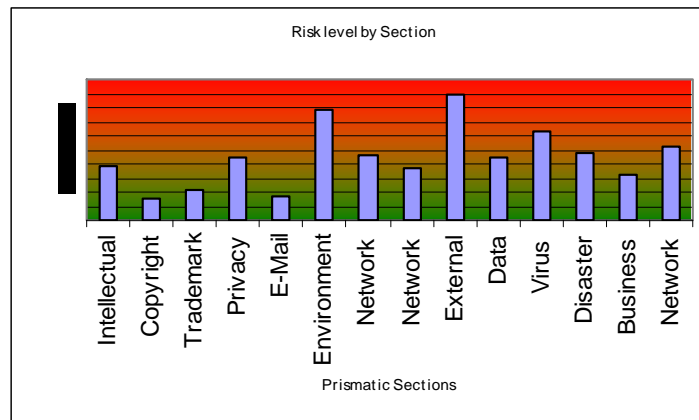
Intellectual Property, Copyright, Trademark, Patent, Privacy, E-mail, Encryption, Contracts, Credit Cards, Data Protection, Environmental Concerns, Network Management, Network Access, External Networks, Data Management and Access, Viruses, Management, and Technical Disaster Recovery

The next version will include: Business Continuity, Network Security, California Privacy and Physical Security. Demonstrating that our product evolves in step with the risks and issues that arise in the ever changing world of the Internet.

There are multiple advantages of using this approach:

- You can rationally establish priorities and more effectively allocate resources across your entire organization.
- You will spend less on a Prismatic® assessment than alternative approaches, allowing you to allocate the cost difference to *fixing* instead of *finding*.
- You have the potential to recover the cost of Prismatic® if your insurance underwriter agrees to fund the assessment as part of your purchase of necessary coverage. And you may find gaps in your coverage that you need to address.

Prismatic® changes the breadth, scope, time frames, and costs of risk assessment. It lets you move money from assessment to remediation and establish priorities and allocate resources based on the full range of risks you face. It provides a better way to address evolving Internet risks.



Prismatic® was designed with today's changing business practices, technology, and standards in mind and it is continually updated to keep pace with the fluctuating environment. Prismatic is offered as a subscription service that provides quarterly updates that incorporate the changing risk landscape.

Since many organizations approach the Internet from multiple directions, with differing objectives and using diverse infrastructures a separate Prismatic® should be used for each business unit. (a "business unit" is a division, subsidiary, or function depending upon your organization's operating structure.) Not only does this approach provide a way to deal with the complexity of larger organizations, it provides a means to assess the differing processes and management practices within the same organization.

# HICOM®

The Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) regulations impose certain requirements on health care providers, payors and clearinghouses in three major area

- Privacy
- Transaction and Code Sets
- Security

Compliance with these regulations is not optional. Where do you stand?

If you don’t know, or are not sure, HICOM can help.

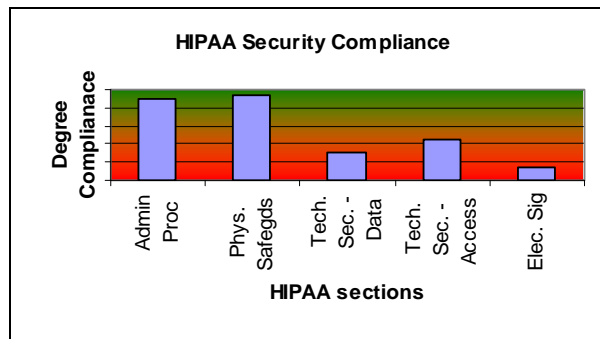
The proprietary process called HICOM (HIPAA Compliance) provides you with a high level compliance assessment report indicating how differing areas should be treated.

- Critical, or high risk, because they are areas in which you are not in compliance and have no plans or programs to achieve compliance
- On track, or medium risk, because your existing plans and programs, if implemented, should be sufficient to ensure compliance; and
- In or near compliance, or low risk.

With this information you can prioritize and plan the most effective way to achieve compliance within the allowed time frame.

## Graphic Summary

Based on your responses to our compliance assessment questionnaire you will get a graphic summary of your compliance level with the privacy, security, and transaction and code set regulations.



## Executive Summary

Findings and recommendations are summarized for each of the major parts of HIPAA legislation and the rationale for determination of your compliance is provided.

## Detail Findings

In addition, a summary is provided for each question that you have answered with comments and recommendations, as appropriate, for actions that you should consider to increase your compliance level within that area.

## Additional offerings

Updates and warnings are provided when new interpretations of regulations or situations arise, an extremely beneficial practice since HIPAA interpretations are constantly evolving and changing.

## ISO 17799

ISO 17799 is the standard for IT security in world wide use.

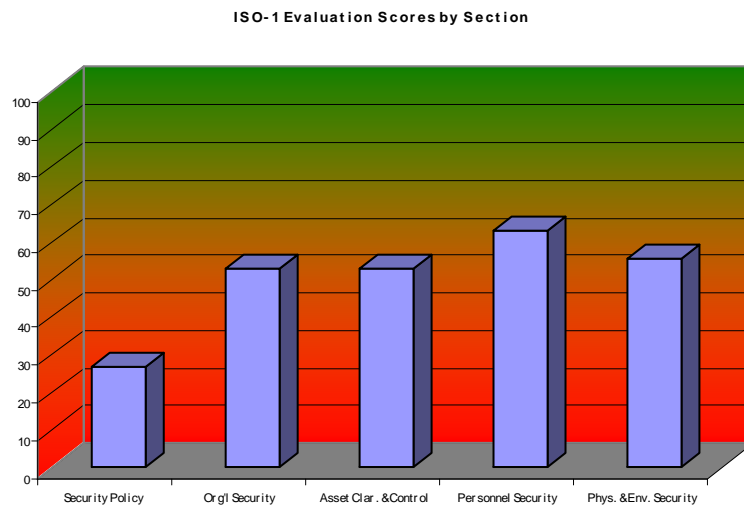
Our protocol address all ten of the areas listed in the standard.

- Security Policy
- Organizational Security
- Asset Clarification and Control
- Personnel Security
- Physical and Environmental Security
- Communication and Operational Management
- Access control
- System Development and Maintenance
- Business Continuity Management
- Compliance

The protocol has over 800 questions, mostly yes/no/I don't know, and can be completed in days by knowledgeable staff.

The resulting report provides you with a roadmap to compliance with ISO 17799, allowing you to set priorities and allocate resources based on your issues.

Larger organizations can have separate assessments done for each of their major business units to compare security across their organization using a common standard.



The graphical exhibit allows you to easily identify areas of concern and to communicate this to all levels of management and staff.

You can use the recommendations in the report to improve your IT security whether or not you apply for certification of compliance with the ISO 17799 standard.

## SD/SLG

(Security Diagnostic for State and Local Governments)

The assessment determines a jurisdiction's readiness level in:

### Internal controls

- Current planning
- Continuity of government and critical services
- Critical infrastructure
- Legal compliance and risk management
- Information sharing and technology
- Operations and information security
- Planning and change management

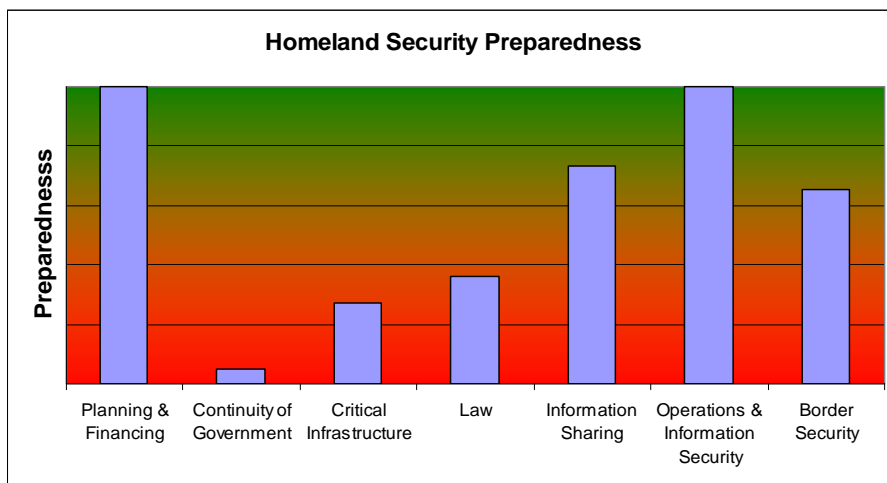
### External infrastructure/assistance/components/needs

- First responders and emergency services
- National Guard
- Local Public Health capabilities to address chemical, biological, and radiological (CBR) risks
- Private sector assistance
- Volunteer service
- School protection
- Homeland Security advisory system
- Public information and communications
- Training, exercising and evaluating
- Mass Casualties Evacuation

The SD/SLG assessment of each of these areas provides you with a readiness/risk profile of your organization that allows you to quickly determine areas of major concern, areas being addressed, and areas needing additional work.

The assessment questionnaire contains over 100 yes/no/don't know questions which are processed through a proprietary automated algorithm to create the risk/readiness profile with recommendations. For larger jurisdictions group summary reports are provided (sample available on request) that will readily identify best practices and problem areas.

The graph below is an extract from the graphical summary



With this assessment as the base, and comparing it to constituent communities a strategic overview of a given jurisdiction's readiness to address the risks that it may face is provided.

# Sarbox

## Sarbanes Oxley Overview

Sarbanes Oxley presents a wide range of issues including legal, technical, processes, document management, and controls assessment and testing.

Our Protocol provides a quick and easy overview of your Sarbanes Oxley compliance in the following areas:

- Auditor Independence
- Corporate responsibilities
- Corporate and criminal fraud accountability
- Corporate Tax returns
- IT Controls

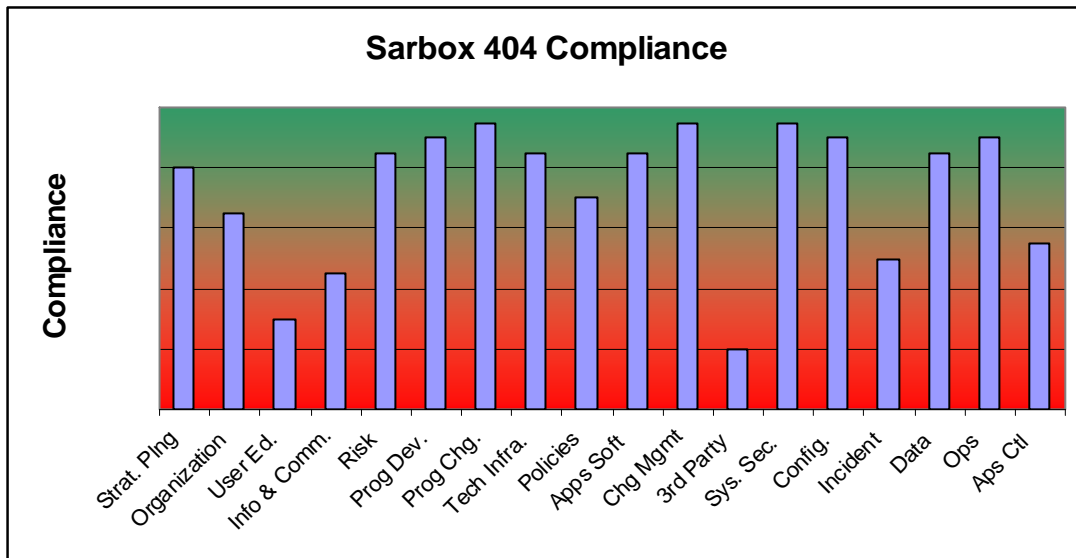
The overview assessment provides a first step in determining at a strategic level if you are in compliance and lets you focus on those areas needing the most work.

Subsections can be used with subsidiaries and divisions to assess the adequacy of their IT controls.

## Sarbanes Oxley Section 404 Compliance

IRM is currently developing Sarbox/404 to address the ongoing need to certify the accuracy and effectiveness of an organization's IT controls. The objective is to provide a report that the client can use to meet their annual IT control review requirement of Sarbanes Oxley section 404. Specifically this area will address the areas of: IT Strategic Planning, IT Organization and relationships, Educate and train users, Information and communication, Risk Assessment, Program development and program change, Technology Infrastructure, Policies and procedures, Application software, Change management, Third Party Services, System Security, Configuration management, Incident management, Data Management, Operations management, Application Controls.

The graphical summary show below will be supported by the detail justification and, where needed, recommendations to address issues found.



This will allow rapid identification of those areas that need to be addressed to meet the annual reporting requirement.

# Supply Chain Risk Assessment

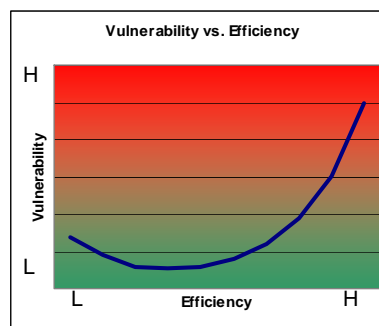
(SCRA)

Supply Chain security and reliability is a continuing concern

- Multiple elements
- Multiple partners
- Multiple geographies
- Multiple political environments
- Compounded by performance and cost pressures
- . . .

A complex, multifaceted problem that evolves and changes in real time, wherein much current effort is devoted to improving process and performance with inconsistent appreciation of the risks that accompany such improvements.

Every supply chain has vulnerabilities. At first a supply chain can become less vulnerable as efficiency improves, however, at some point improvements in efficiency bring ever increasing vulnerabilities. The objective is to understand when improvements dramatically affect vulnerabilities.



IRM used our ASAP technology to create a strategic level assessment approach that is:

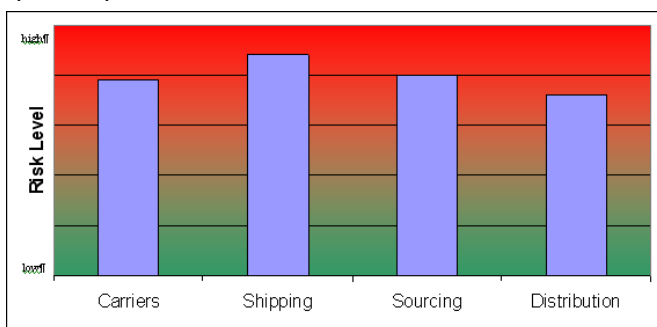
- Easy to use, Applicable to broad range of issues, clients and industries, Focused on identifying strategic level risk and security issues providing guidance to address the issues found, Repeatable, Adaptable and evolves with change, and economical

SCRA consists of five major sections:

- Domestic (US) Transportation, International Transportation, Procurement, Storage and Distribution, and Financial Considerations

With over 130 questions that will evolve as new issues, risk, business models and practices change.

Output Report



- Graphic Risk Summary by Section
- Detailed response recommendations (average report 20 + pages)
- Electronically transmitted in PDF format within two business days

## Training

The protocols<sup>1</sup> can be used in concert with training programs in the following ways:

- Prior to the training as a way to gauge the attendees knowledge and awareness of the topic under discussion.
- By providing the output report to the attendees prior to the meeting one can reinforce the need for the training and identify areas wherein the trainee needs to be better informed.
- Identify areas that need special attention in the training.
- Provide a bench mark against which to measure the impact of the training
- Build a database of awareness on various topics
- Use the findings in graphical summaries to reinforce the necessity for the training in the introductory session.

At the end of the training session the attendees take the questionnaire again and use the findings to:

- Demonstrate the increased awareness and knowledge to the corporate sponsor
- Provide personalized report back to the attendees
- Use the findings in graphical summaries to demonstrate the impact of the training.

In addition, while the protocols are straightforward and require little training for their use, there exist guides and teleconference assistance which can be provided. For larger programs instructors are available for on site training the cost of which will depend upon the specifics of the situation. Some clients have found the protocols to be an effective means of proactive awareness training.

## Custom Applications

The underlying technology behind the protocols can be used to create tailored assessments and reports on topics of specialized interest. By using the ASAP formats, focused questionnaires, and output reports a customized application can be created in a timely and economical fashion. Some examples of this approach are:

- Specialized risk assessments internal to an organization that focus on proprietary activities and metrics.
- Assessments of specialized business partner activity when a large number of business partners are involved.
- Gathering of information from business partners, customers and other interested parties on focused topics.

If you have a special situation where you think this approach might be of help give us a call and we will be happy to discuss ways to assist you.

---

<sup>1</sup> The protocols are the specific offerings listed in this document.

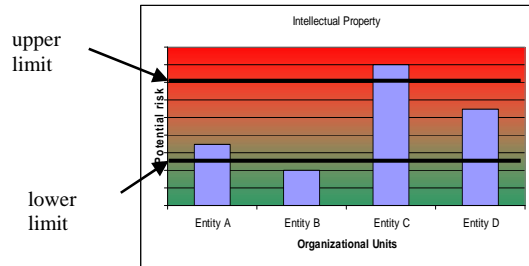
# Group Reports

These graphic summaries provide organization wide guides. They are abstracted to present reporting alternatives and can be used with all protocols if appropriate to the client situation.

There are three basic reports:

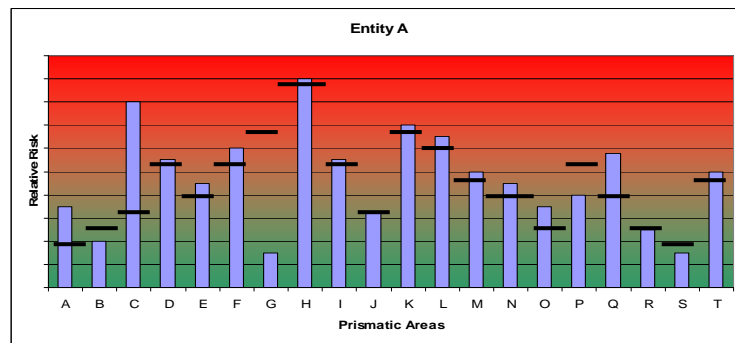
**Relative Risk Report**—Rating across each business unit including established risk levels (acceptable to immediate review)

You establish, based on your organizations appetite for risk, upper and lower risk limits by area. This allows easy identification of those entities (business units) that are beyond what you have set as an acceptable risk level and those that are below the lower limit represent best practice. In this example Entity C needs an immediate review of their intellectual property practices. The recommendations in their report will provide the beginnings of a task plan.



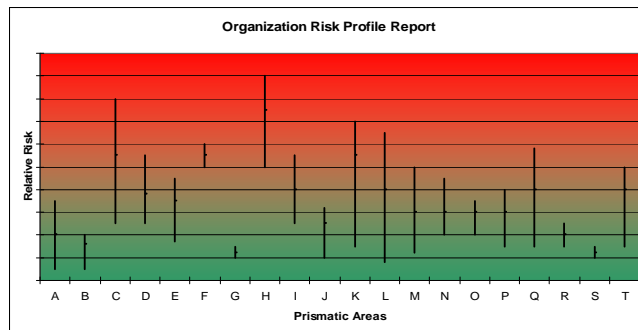
**Business Unit Profile Report**—All risk by a business unit compared to organization averages

The dash — represents the organization wide average. This allows rapid identification of areas that need immediate attention and areas that may represent best practice and should be reviewed for organizational wide use. E.g. Area C is worse than average, while area G much better than average. And everyone is at high risk in area H.



**Organization Risk Profile**—High/low/average for each risk area

This report provides an at a glance overview of the organizations risk profile. It allows a rational for the setting of priorities and the allocation of resources. e.g. Area H has the highest average and no one seems to be addressing it in a satisfactory manner. While areas G & S find the entire organization operating at low risk levels. This report can be used to communicate plans at the highest level of the organization.



These reports help identify issues, establish priorities, & allocate resources. They can also be used to shorten assessment cycle getting to remediation faster.

The reports are optional and not part of the standard report as they only apply to larger organizations.

## Application and Usage

The NRG family of protocols can be used in many ways. Some examples follow:

Strategic Input. Examining the broad spectrum of risk and compliance issues provides substantial input in creating a strategy.

Resource Allocation and Priority Setting. The graphical summaries can be used to determine which areas require immediate attention and which can wait.

They provide a second opinion at reasonable cost

Merger & Acquisition. Can be used as part of the due diligence process.

Operational Validation. Verify the progress or status of a situation quickly and inexpensively.

Keeping up with change. Subscription products allow you to measure progress and to keep up with evolving risks.

Insurance. Can be used as input in determining which risks may require coverage and which are acceptable

## Contact Information

Doug Nagan  
Nagan Research Group LLC  
32 Lobb Lane  
Deep River, CT 06417  
203-987-8946  
[doug@naganresearchgroup.com](mailto:doug@naganresearchgroup.com)