
Final Version of Initial Report

SG-SBP

SBP/07-0049

Revision 1.1
February 8, 2008

# RECOMMENDATION FOR CREATING A COMPREHENSIVE FRAMEWORK FOR RISK MANAGEMENT AND COMPLIANCE IN THE FINANCIAL SERVICES AND INSURANCE INDUSTRIES



Printed in the United States of America

Prepared by the members of SG-SBP

# DOCUMENT STATUS

Revision 1.1 – February 8, 2008

in080049

Secretariat
Information Technology Industry Council

INCITS Final Report
for Information Technology

# RECOMMENDATION FOR CREATING A COMPREHENSIVE FRAMEWORK FOR RISK MANAGEMENT AND COMPLIANCE IN THE FINANCIAL SERVICES AND INSURANCE INDUSTRIES

## Abstract

This report describes the findings and recommendations of the INCITS Study Group for Security Best Practices regarding the direction that formal standards must take to support the Financial Services and Insurance industries. Of the many possibilities to be considered, the Study Group decided to focus on a security aspect that is rapidly growing in difficulty and would have a feasible resolution with the greatest beneficial impact on the two industries. That aspect embraces information security risk management and compliance. This recommendation includes a comprehensive overview of the critical standards that already exist, identifies the most serious gaps, and makes recommendations regarding the actions that should be taken and the organizations that could best take the lead in filling these gaps. It is anticipated that the study of needs in the financial services and insurance industries will lead to changes in the INCITS program of work such that it can be assured that Information and

Communications Technology (ICT) standards are successfully meeting the broad needs of all their user communities.

# Points of Contact:

**SG-SBP Chair**
Ed Stull
sponsored by:
Direct Computer Resources, Inc.
20600 Georgia Avenue
Brookeville, MD 20833
estull@datavantage.com
Tel: 301 260-1781

**Web Site**
www.incits.org/tc_home/sbp.htm

**Reflector**
incits-sbp@lyris.itic.org

**SG-SBP Vice Chair Financial Services**
Mark Clancy
SVP, IT Risk Management
Citigroup
111 Wall Street
19th Floor
New York, NY 10005
Ofc: 212-657-3568

**SG-SBP Vice Chair Insurance**
Robert Talbot
VP, Information Security
Coventry Health Care
4141 N. Scottsdale Rd.
Scottsdale, AZ 85251
Ofc: 480-445-4848

**Secretary**
Nadya Bartol
Sr. Associate
Booz Allen Hamilton
8283 Greensboro Drive
McLean, VA 22102
Ofc: 703-377-1252

**Final Report Editor**

Aaron McPherson
Practice Leader
Financial Insights, an IDC Company
5 Speen Street, Framingham
Framingham, MA 01701
Ofc: 508-935-4670
Email: amcpherson@financial-insights.com

**INCITS Secretariat**

Administrator Standards Processing
1250 Eye Street, NW
Suite 200 Washington, DC 20005

Tel: 202-737-8888

Fax: 202-638-4922
Email: incits@itic.org

Contents Page

## Foreword

This report describes the findings and recommendations of the INCITS Study Group for Security Best Practices regarding the direction that formal standards must take to support the Financial Services and Insurance industries. Of the many possibilities to be considered, the Study Group decided to focus on a security aspect that is currently growing rapidly in difficulty and would have a feasible resolution with the greatest beneficial impact on the two industries. That aspect embraces information security risk management and compliance. This recommendation includes a comprehensive overview of the critical standards that already exist, identifies the most serious gaps, and makes recommendations regarding the actions that should be taken and identifies the organizations that could best take the lead in filling these gaps.

There are doubtless many other relevant standards and frameworks that could be usefully discussed in the context of this report; the ones included are those that the Study Group members were most familiar with and that we judged most significant in the financial services and insurance industries. We encourage other groups with similar objectives to use this report as a foundation on which to build broader, more comprehensive surveys. One potential area of expansion, for example, would be the establishment of a formal taxonomy of risks, which could be used to index standards in a systematic way.

It is anticipated that the study of needs in the financial services and insurance industries will lead to changes in the INCITS program of work such that it can be assured that Information and Communications Technology (ICT) standards are successfully meeting the broad needs of all their user communities.

This document is not an American National Standard and the material contained herein is not normative in nature. Comments on the content of this document should be sent to the INCITS Secretariat,

Information Technology Industry Council, 1250 Eye Street, NW (Suite 200), Washington, DC 20005.

Participants in the Study Group for Security Best Practices (SG-SBP) that made significant contributions were (alphabetically):

Nadya Bartol
Ken Belva
Dan Benigni
Joe Buonomo
Jean-Pierre Champigny
Mark Clancy
Russ Davis
Scott Erkonen
John Fricke
Mike Gerdes
Richard Gomes
Christine Knibloe
Micki Krause
Aaron McPherson
Ed Stull
Robert Talbot
Tom Wehrle
Preston Wood

## Introduction

As directed by the INCITS Executive Board on July 20, 2007, a study group was chartered to produce a recommendation on Security Best Practices for the Financial Services and Insurance industries. This document represents the fulfillment of that charter.

In the course of its work, the Study Group decided to focus specifically on the issues of risk management and compliance, as this was where the greatest opportunity for improvement existed. This report focuses on issues with respect to the policies, practices and deployment of risk management services and controls in the context of compliance requirements and controls. The report does not focus on specific technology-oriented standards, such as those for key management or biometrics, or specific requirements for specific devices that may be leveraged within and beyond the financial services and insurance industries. Given competitive pressures, public reactions and profitability goals, a good risk management program requires a strong strategic focus on a business, and must be accomplished in conjunction with a robust compliance program that ensures that measures are in place to correctly articulate and manage risk within the capabilities and resources of that business. Considerations of where we are today, where we are going and where we want to be are examined. As stated earlier, it is anticipated that this study will lead to changes in the INCITS program of work such that it can be assured that ICT standards are successfully meeting the broad needs of all their user communities.

The report that follows is divided into three main sections:

Section 1 describes the existing standards landscape, including consortia, standards bodies, and the commonly accepted standards that are utilized today. It notes where differing but parallel standards are followed in the financial services and insurance industries, and where the industries do, and do not, share a commonly accepted standard.

Section 2 lays out the recommendations of the Study Group, based on the findings of Section 1. These include actions to fill gaps in the existing set of standards, reconcile differences in standards between industries (where there is good reason to do so), and update standards to eliminate ambiguity, overlaps, contradictions, and obsolete references. For each recommendation, the report will specify which organization it believes is best suited to lead the work effort.

Section 3 provides a summary of the Study Group and its operations.

# 1. EXISTING STANDARDS LANDSCAPE

At the time of publication, the editions of the standards referenced in the text were valid. All standards are subject to revision, and parties to agreements based on this standard are encouraged to investigate the possibility of applying the most recent editions.

## 1.1. FINANCIAL SERVICES STANDARDS

The financial services industry does not have any one framework for information security or technology risks management that is widely in use or that is tailored to the industry itself. The IT Risk/ Information security standards specific to financial services that have been widely adopted are generally limited to an individual sub-domain and/or technical area for example cryptographic key management for ATM machines versus the overall IT risk management umbrella.

The current state of practice is to use a combination of IT industry benchmarks and then augment those to meet specific additional requirements set forth by governmental regulatory agencies or self regulating bodies. Each financial institution may have its own active project to create a mapping document to reference control requirements between one or more external standards to their own current or "go to" version of IS/IT polices & standards, with multinationals doing this for each of the major countries in which they operate.

The standards in use by financial institutions reviewed by this study group all can be loosely grouped into three categories; Compliance Frameworks, Risk Management Models, and Maturity Models. The group noted the existence of many excellent and mature standards that focus on specific technologies and devices, such as those developed by the X9 group or the PCI standard. Due to the

declared focus on risk management and compliance these standards were considered outside of the scope of the group's work. Only a few of the reference works from the study group work incorporate features from more than a single category, which places the burden of integrating the different elements into a cohesive risk management program on financial institutions and other adopting organizations.

**Compliance Frameworks**

The major driver for the financial services industry on the regulatory front is based upon the examination handbook produced by the Federal Financial Institutions examination Council (FFIEC) in the US and either COBIT or ISO/IEC 27001/27002 internationally. The FFIEC material is written as a guide to the regulatory examiners and has in a sense been "reverse engineered" by financial institutions to define their policies and practices. While the FFIEC has a significant overlap with the ISO/IEC 27002 in terms of control requirements each work advocates some control sets that the other is silent on. Standards based compliance frameworks in use by financial institutions include: ISO/IEC 27001/27002, NIST 800-53, and COBIT. While it is sometimes overlooked by those in the information security area, IT service management is becoming more recognized as an integral part of information security programs. As a result there is also growing interest in the adoption of ITIL v3 and ISO/IEC 20000 frameworks by institutions focused on the integration of information security and operational IT management.

**Maturity Models**

There are also a number of maturity models (ISM3, ISO/IEC 21827, and SOMA) and measurement-related standards (NIST SP 800-55 and ISO/IEC 27004) that have been developed or are under development for measuring effectiveness of information security controls and processes. These models use a mix of control statements and requisite practices to define the maturity level and some also offer frameworks for developing metrics to measure the

maturity level and to quantify effectiveness of information security controls and processes. Results of implementation of maturity models and measurement frameworks can provide input into both compliance and risk management decisions.

**Risk Management Models**

There are a number of standard Risk Management and/or risk assessment models that are available, but these are infrequently used by financial institutions if in-house models either pre-date the external standards or model risk in a fashion more tailored to an individual organization. The common component of these models is they produce risk measures that are stratified into high, medium, and low risk designations. Some models also separately advocate or delineate confidentiality, integrity, and availability risks for the target assets\processes. Each model has its own generalized approach to compute the risk using asset values, threat, vulnerability, impact, and likelihood with the biggest difference being how likelihood is addressed.

In models like NIST 800-30 likelihood is a measure of control effectiveness to a given adversary where as in FAIR & COSO it is a frequency of loss driver and in ISO/IEC 27005 and OCTAVE it is a probability of a threat scenario occurring. The various models also use either quantified measurements of likelihood and/or subjective measurements. None of the models deal elegantly with the combination of quantitative regression analysis of internal and external data and subjective "look forward" analysis to produce a blended likelihood based upon input from subject matter experts in the institution. The main limitation of the quantitative methods is a lack of a rich data set to establish frequency of events.

It is also worth noting there are additional risk management requirements upon financial institutions through other standards compacts, but these were not reviewed as part of the Study Group effort. An example would be the Bank of International Settlements' Basel II accord which addresses capital and operational risks. This risk

management accord clearly has some intersection between the IT/IS standards frameworks discussed here as Information Technology Risks align to a sub-set of operational risks and will need to integrate with IT risk management models and is unclear as how it will incorporate the controls frameworks and maturity models.

**State of the industry**

Financial institutions that use any standards based compliance framework frequently use ISO/IEC 27001/27002 along with a regulatory reference like FFIEC to develop their own polices and standards. Additionally some institutions have been incorporating the COSO, ISM3, SOMA, and/or COBIT control frameworks to put additional context around the FFIEC and ISO/IEC 27002 control sets in terms of maturity. There is not a lot of standardization on the risk management models as many institutions are still utilizing home grown models for information security that closely map to their compliance based policy frameworks. The main economic driver for control frameworks is with address compliance issues and to some degree risk management considerations have been at best secondary.

There is little apparent linkage between the compliance frameworks and the outputs of risks assessments, and as such, the application of controls is sometimes asymmetrical to the risks of the assets. The example often discussed is the controls stipulated in the control frameworks to protect a single customer record is identical to the controls to protect several million records, while, from a risk perspective, these situations are quite dissimilar. By not discriminating when controls are applied, unneeded expense is directed to protection of assets for the sake of compliance where risk is modest and additional expense is not directed to areas that are compliant to the standard, but may warrant additional control expense because the risk is significant.

Institutions are also using the maturity modeling models as a method to rationalize current state and forecasted future state. This has been

becoming increasingly important due to the rapid changes in the threat environment and the increased sophistication of adversaries. Many efforts are introduced to address tactical concerns with the "information security risk of the moment" and the maturity modeling allows institutions to put those investments in the context of a longer range plan for maturing controls in a given area. This has also proven helpful to institutions in describing their approach, objectives, and to some degree priorities to regulatory agencies in an objective manner

### 1.1.1. FINANCIAL INSTITUTION SPECIFIC STANDARD – COMPLIANCE FRAMEWORK - FFIEC INFORMATION SECURITY EXAMINATION HANDBOOK

**Description:** The Information Security booklet provides guidance for examiners and financial institutions to use in identifying information security risks and evaluating the adequacy of controls and applicable risk management practices of financial institutions.

The safety and soundness of the financial industry and the privacy of customer information depend on the security practices of banks, thrifts, credit unions and their service providers. The Information Security Booklet describes how an institution should protect the systems and facilities that process and maintain information. The booklet calls for financial institutions and technology service providers to maintain effective programs tailored to the complexity of their operations.

Status: Complete
Controlling Organization: Federal Financial Institutions Examination Council
Contact Information: http://www.ffiec.gov/
URL: http://www.ffiec.gov/ffiecinfobase/booklets/information_security/information_security.pdf

## 1.2. INSURANCE INDUSTRY STANDARDS

Although the many components of the insurance industry are classified as a single vertical, primarily based upon coverage by contract whereby one party undertakes to indemnify or guarantee

another against loss by a specified contingency or peril, the industry itself is fragmented and personified by the risk being addressed under contract (Merriam-Webster dictionary). The industry is characterized by multiple risk models and loss underwriting rules that incorporate many variables, such as group demographics, geographic location, and individual and group measurements, as well as valuation and loss/risk sharing. The industry is primarily composed of the following groupings, each with its own risk modeling:

- Accident Insurance
- Health Insurance (including models such as Individual Healthcare, PPO, HMO, Government sponsored programs, and Health Savings Accounts)
- Life Insurance (Term and Whole Life)
- Property and Casualty (including Homeowners, Landlord, Vehicle, etc.)
- Title Insurance
- Unemployment Insurance
- Workers Compensation Insurance
- Re-Insurance (shared risk)

The diversity of the industry and the proliferation of authoritative regulatory government bodies at federal and state levels add to the complexity of industry compliance. In general all regulatory and statutory guidelines and mandates require risk assessment as a core competency of the risk management framework used within the insurance industry, however, the specifics of the framework are in fact left to the individual company to ascertain and implement. In addition to the information security specific regulatory requirements, the insurance industry has an additional burden of providing, ensuring and reporting on the privacy aspects of customer health and personally identifiable information to ensure compliance with state and federal privacy regulations, such as the Health Insurance Portability and Accountability Act (HIPAA).

The insurance industry vertical is a risk based business. As such the relative immaturity of industry specific information security risk assessment and compliance standards is somewhat surprising. This is true for both US domestic standards, as well as international standards.

Prior to the year 2000 there were relatively few information security or privacy statues or regulations applying to the industry, GLBA and HIPAA being the exceptions. Since that date, additional statues and regulations have been instituted at the state level in nearly all 50 states, and those not currently included are contemplating or have proposed legislation specifically addressing information security and privacy considerations. Political considerations aside, the legislative environment can be currently considered to be hostile to the industry in general and trending towards more consumer friendly protection activities. Enforcement of compliance is increasing, with the authoritative agencies developing their individual compliance frameworks and standards, as well as requiring regulatory specific auditing for compliance.

The increasing risks in the industry vertical that must be considered when measuring risk and compliance includes public perception of information security as a competitive advantage or disadvantage in direct to consumer sales and contract processes. The trending across all industry verticals in the contract process is to include vendor regulatory or best practice compliance contract terms, with linked contract non-compliance remedies and liabilities. Information security compliance or lack thereof, has a direct mapping to business lost opportunity costs, beyond normal direct and indirect cost considerations.

The evaluation of risk and compliance assessments, to include regulatory reporting, is burdensome without an integrated standard or framework. As with the financial services sector the companies within the various aspects of the insurance industry have in most cases attempted to leverage a composite model of standards for assessment, compliance and risk management, with the publication

of ISO 27001/27002 taking the lead as the standard to be considered whenever the requirement for a standard is called out. Internationally, depending upon the host country, a company doing business as an insurer may be considered a financial services entity and significant changes in the regulatory landscape, such as Basel II, have driven competitive advantage to those companies mapping the controls framework to the regulation and which are in compliance with the regulations. US Domestic and international consolidation within the insurance vertical through merger and acquisition, as well as the commoditization of insurance business models through shared services, have inflated the costs associated with compliance and risk management. Cross-border arrangements have magnified the complexity of attempting to define a common framework with no authoritative standard.

As with the financial services industry, the current standards in use are categorized in the same manner; compliance frameworks, risk management frameworks and models, and maturity models.

**Compliance Frameworks**

At the US domestic national level, two primary regulatory drivers forced the inclusion of assessment and compliance into the business risk model. First, with the introduction of the Sarbanes-Oxley act (SOX) and its applicability to publicly held companies, COSO/COBIT became a consideration in the information security controls framework. This extension of the compliance framework elevated the visibility of risk assessment as a business risk function and further, also incorporated the concept of standardized process under the standardized IT environmental management control structure as a risk. External audit controls definition and normative control modeling (financial risk based) has forced maturity of the security/privacy function and incorporated the concepts of pervasive and entity controls at the Board of Directors level within publicly-held companies. Secondly, for those companies storing or managing healthcare specific information, HIPAA, with its specific security and privacy rules, has mandated a general compliance

framework within which companies must demonstrate compliance and are subject to monetary damages when found non-compliant, not to mention the damage to reputation derived from a non-compliant finding.

At the US domestic state level, the drivers for a common standard and framework are many and are extended to Personally Identifiable Information (PII) in an attempt to legislatively attribute risk and cost associated with identity theft. While the data attributes covered within the legislative activity are fairly specific and have a commonality, there is a dearth of legislative guidance related to the controls framework required. It is left to the individual organizations to derive acceptable controls based on business risk and associated costs.

**Maturity Models**

When used, the companies within the insurance industry make use of the same models as articulated in the financial services section.

**Risk Management Models**

Although the models identified as being used within the financial services sector are also used somewhat in the insurance sector, trends within the insurance industry are to draw tighter integration between business resiliency, business risk and information security risk. The risk appetite of the company in question will broadly define thresholds for risk assessment and materiality The challenges presented by the generally accepted risk assessment methodologies is that they require a high degree of knowledge of both business model and risk assessment discrimination, also known as common sense. Each of the methodologies also present the challenge of interpreting discrete results and presenting those results in terms easily understood and digestible by business leaders, else they become non-actionable.

The recently published OCTAVE-Allegro risk assessment model incorporates a higher degree of business impact consideration

within the model and supports the industry risk assessment and analysis trends, as well as articulating risk in terms of business impact. The Octave-Allegro approach "is designed to allow broad assessment of an organization's operational risk environment with the goal of producing more robust results without the need for extensive risk assessment knowledge. This approach differs from previous OCTAVE approaches by focusing primarily on information assets in the context of how they are used, where they are stored, transported, and processed, and how they are exposed to threats, vulnerabilities, and disruptions as a result." Information asset valuation is derived directly from business input. The Allegro methodology allows for integrating business resiliency concepts such as driving business decisions related to business continuity / crisis management and disaster recovery objectives.

While publication of the Allegro methodology is a step forward in the ability to provide actionable results, the disconnect or lack of integration between standards related to Compliance Frameworks, Maturity Models, and Risk Management Models still exists and must be reconciled before a true risk and compliance picture can be presented.

**State of the Industry**

To reiterate, the process to reconcile "the disconnect" between the standards addressing the three components of compliance and risk management identified in this document is complex and time consuming. Organizations within the insurance vertical tend to make use of one standard methodology in one of the categories and, rather than attempting to perform reconciliation, develop in-house custom standards to address the remaining components. The proliferation of legislative activity makes compliance a moving and shifting target that must be constantly monitored and re-evaluated. A primary driver of the legislation is impact upon the consumer and the increasing cost of fraud and identity theft, to include medical identity.

The granularity of the controls thresholds and business valuation (materiality) has been and will continue to be a challenge. Because of this complexity in the environment and lack of reconciliation between the standards many insurance industry security programs are driven by current hot topics or public relations risks. In order to rationalize the risk beyond a conceptual level, and to provide and communicate business value that is traceable to compliance and risk mitigation, a common standard integrating the components should be contemplated.

No sector specific standards were identified.

## 1.3. COMMON STANDARDS BETWEEN FINANCIAL SERVICES AND INSURANCE INDUSTRIES

The bulk of the information security and risk management standards that are published are not industry specific and have been utilized to different degrees in both the Financial Services and Insurance sectors.

### 1.3.1. ISO/IEC 27001:2005

**Description**: ISO/IEC 27001:2005 specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System within the context of the organization's overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof.

ISO/IEC 27001:2005 is designed to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties.

ISO/IEC 27001:2005 is intended to be suitable for several different types of use, including the following:

- use within organizations to formulate security requirements and objectives;
- use within organizations as a way to ensure that security risks are cost effectively managed;
- use within organizations to ensure compliance with laws and regulations;
- use within an organization as a process framework for the implementation and management of controls to ensure that the specific security objectives of an organization are met;
- definition of new information security management processes;
- identification and clarification of existing information security management processes;
- use by the management of organizations to determine the status of information security management activities;
- use by the internal and external auditors of organizations to determine the degree of compliance with the policies, directives and standards adopted by an organization;
- use by organizations to provide relevant information about information security policies, directives, standards and procedures to trading partners and other organizations with whom they interact for operational or commercial reasons;
- implementation of business-enabling information security;
- use by organizations to provide relevant information about information security to customers.

Status: Complete
Controlling Organization: International Organization for Standardization
Contact Information: http://www.iso.org/iso/support/contact_iso.htm
URL: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103

### 1.3.2. ISO/IEC 27002:2005

**Description**: ISO/IEC 27002:2005 establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. The objectives outlined provide general guidance on the commonly accepted goals of information security management. ISO/IEC 27002:2005 contains best practices of control objectives and controls in the following areas of information security management:

- security policy;
- organization of information security;
- asset management;
- human resources security;
- physical and environmental security;
- communications and operations management;
- access control;
- information systems acquisition, development and maintenance;
- information security incident management;
- business continuity management;
- compliance.

The control objectives and controls in ISO/IEC 27002:2005 are intended to be implemented to meet the requirements identified by a risk assessment. ISO/IEC 27002:2005 is intended as a common basis and practical guideline for developing organizational security standards and effective security management practices, and to help build confidence in inter-organizational activities.

Status: Complete
Controlling Organization: International Organization for Standardization
Contact Information: http://www.iso.org/iso/support/contact_iso.htm
URL: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50297

### 1.3.3. INFORMATION SECURITY MANAGEMENT MEASUREMENT – ISO/IEC 27004

**Description:**[1] ISO/IEC 27004 will provide guidance on the development and use of effective measures and measurement of the Information Security Management System (ISMS) established by ISO/IEC 27001, including the ISMS policy, objectives and security controls in the Statement of Applicability used to implement and manage information security. It provides management a methodology to determine ISMS effectiveness and guidance on how organizations can determine adequacy of the policy, risk management, control objectives, controls, processes and procedures of an ISMS. The implementation of this standard enables organizations to create an Information Security Measurement Program (ISMP) to assist management in determining the adequacy of controls and prioritizing the continuous improvement action needed to maintain them. The current draft standard also includes additional guidance to help organizations with:

- Developing measures;
- Implementing and operating an Information Security Measurement Program;
- Collecting, analyzing, and communicating measures to stakeholders;
- Using collected measures to support decisions related to the ISMS;
- Using collected measures to improve ISMS control objectives and controls;
- Facilitating continuous improvement of the ISMS and ISMP

Status: Under Development. Standard is normalized with ISO/IEC 15939, System and Software Measurement and has received substantial contribution based on NIST SP 800-55.
Controlling Organization: JTC 1/SC 27
Contact Information: http://www.iso.org/iso/iso_technical_committee.html?commid=45306
URL: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42106

[1] Portions of the description of ISO/IEC 27004 extracted from ISO/IEC 27004 Comment Draft 3 (CD 3) - dated November 11, 2007

### 1.3.4. INFORMATION TECHNOLOGY — SECURITY TECHNIQUES — INFORMATION SECURITY RISK MANAGEMENT (ISO/IEC 2ND FCD 27005)

**Description**: This International Standard provides guidelines for Information Security Risk Management in an organization, supporting in particular the requirements of an ISMS according to ISO/IEC 27001. However, this International Standard does not provide any specific methodology for information security risk management. It is up to the organization to define their approach to risk management, depending for example on the scope of the ISMS, context of the risk management, or industry sector. A number of existing methodologies can be used under the framework described in this International Standard to implement the requirements of an ISMS. This International Standard is relevant to managers and staff concerned with information security risk management within an organization, and, where appropriate external parties supporting such activities.

Status: Under Development
Controlling Organization: JTC 1/SC 27
Contact Information: http://www.iso.org/iso/iso_technical_committee.html?commid=45306
URL: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42107

### 1.3.5. INFORMATION TECHNOLOGY -- SECURITY TECHNIQUES– SYSTEMS SECURITY ENGINEERING – CAPABILITY MATURITY MODEL (SSE-CMM®) (ISO/IEC FDIS 21827)

**Description:** A wide variety of organizations practice security engineering in the development of computer programs, whether as operating systems software, security managing and enforcing functions, software, middleware or applications programs. Appropriate methods and practices are therefore required by product developers, service providers, system integrators, system administrators, and even security specialists. Some of these organizations deal with high-level issues (e.g., ones dealing with

operational use or system architecture), others focus on low-level issues (e.g., mechanism selection or design), and some do both. Organizations may specialize in a particular type of technology or a specialized context (e.g., at sea).

The SSE-CMM® is designed for all these organizations. Use of the SSE-CMM® should not imply that one focus is better than another or that any of these uses are required. An organization's business focus need not be biased by use of the SSE-CMM®.

Based on the focus of the organization, some, but not all, of the security engineering practices defined will apply. In addition, the organization may need to look at relationships between different practices within the model to determine their applicability. The examples below illustrate ways in which the SSE-CMM® may be applied to software, systems, facilities development and operation by a variety of different organizations.

This International Standard has a relationship to ISO/IEC 15504, particularly ISO/IEC 15504-2, as both are concerned with process improvement and capability maturity assessment. However, ISO/IEC 15504 is specifically focused on software processes, whereas the SSE-CMM® is focused on security. This International Standard has a closer relationship with the new versions of ISO/IEC 15504, particularly ISO/IEC 15504-2, and is compatible with its approaches and requirements.

Status: Complete
Controlling Organization: JTC 1/SC 27 and International System Security Engineering Association (ISSEA)
Contact Information: http://www.iso.org/iso/iso_technical_committee.html?commid=45306
http://issea.org
URL: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=44716
http://sse-cmm.org

### 1.3.6. RECOMMENDED SECURITY CONTROLS FOR FEDERAL INFORMATION SYSTEMS (NIST 800-53)

**Description:** The purpose of this publication is to provide guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the federal government. The

guidelines apply to all components of an information system that process, store, or transmit federal information. The guidelines have been developed to help achieve more secure information systems within the federal government by:

- Facilitating a more consistent, comparable, and repeatable approach for selecting and specifying security controls for information systems;
- Providing a recommendation for minimum security controls for information systems categorized in accordance with Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems;
- Promoting a dynamic, extensible catalog of security controls for information systems to meet the demands of changing requirements and technologies; and
- Creating a foundation for the development of assessment methods and procedures for determining security control effectiveness.

Status: Complete
Controlling Organization: National Institute of Standards and Technology
Contact Information:
Public Inquiries Unit
NIST, 100 Bureau Drive, Stop 1070, Gaithersburg, MD 20899-1070
Email: inquiries@nist.gov
Phone: (301) 975-NIST (6478) or TTY (301) 975-8295
URL: http://csrc.nist.gov/publications/nistpubs/800-53/SP800-53.pdf

### 1.3.7. RISK MANAGEMENT GUIDE FOR INFORMATION TECHNOLOGY SYSTEMS (NIST 800-30)

**Description:** Risk is the net negative impact of the exercise of a vulnerability, considering both the probability and the impact of occurrence. Risk management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level. This guide provides a foundation for the development of an effective risk management program, containing both the definitions and the

practical guidance necessary for assessing and mitigating risks identified within IT systems. The ultimate goal is to help organizations to better manage IT-related mission risks.

In addition, this guide provides information on the selection of cost-effective security controls. These controls can be used to mitigate risk for the better protection of mission-critical information and the IT systems that process, store, and carry this information. Organizations may choose to expand or abbreviate the comprehensive processes and steps suggested in this guide and tailor them to their environment in managing IT-related mission risks.

Status: Complete
Controlling Organization: National Institute of Standards and Technology
Contact Information:
Public Inquiries Unit
NIST, 100 Bureau Drive, Stop 1070, Gaithersburg, MD 20899-1070
Email: inquiries@nist.gov
Phone: (301) 975-NIST (6478) or TTY (301) 975-8295
URL: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

### 1.3.8. PERFORMANCE MEASUREMENT GUIDE FOR INFORMATION SECURITY (NIST 800-55R1)

**Description:** A number of existing laws, rules, and regulations—including the Clinger-Cohen Act, the Government Performance and Results Act (GPRA), the Government Paperwork Elimination Act (GPEA), and the Federal Information Security Management Act (FISMA)—cite information performance measurement in general, and information security performance measurement in particular, as a requirement. In addition to legislative compliance, agencies can use performance measures as management tools in their internal improvement efforts and link implementation of their information security programs to agency-level strategic planning efforts.

The following matters must be considered during development and implementation of an information security measurement program:

- Measures must yield quantifiable information (percentages, averages, and numbers);

- Data that supports the measures needs to be readily obtainable;
- Only repeatable information security implementation processes should be considered for measurement; and
- Measures must be useful for tracking performance and directing resources.

The measures development process described in this document ensures that measures are developed with the purpose of identifying causes of poor performance and point to appropriate corrective actions.

This document focuses on the development and collection of three types of measures:

- Implementation measures to measure execution of security policy;
- Effectiveness/efficiency measures to measure results of security services delivery; and
- Impact measures to measure business or mission consequences of security events.

Status: Existing guide in place, Revision 1 is an update of the existing guide to align with NIST SP 800-53 control set. Measures development and implementation processes defined in the document are applicable beyond NIST control sets.
Controlling Organization: National Institute of Standards and Technology
Contact Information:
Public Inquiries Unit
NIST, 100 Bureau Drive, Stop 1070, Gaithersburg, MD 20899-1070
Email: inquiries@nist.gov
Phone: (301) 975-NIST (6478) or TTY (301) 975-8295
URL: http://csrc.nist.gov/publications/drafts/800-55-rev1/draft-sp800-55-rev1.zip

### 1.3.9. INFORMATION SECURITY HANDBOOK – A GUIDE FOR MANAGERS (NIST SP 800-100)

**Description:** The Information Security Handbook provides a broad overview of information security program elements to assist managers in understanding how to establish and implement an information security program. Typically, the organization looks to the

program for overall responsibility to ensure the selection and implementation of appropriate security controls and to demonstrate the effectiveness of satisfying their stated security requirements. The topics within this document were selected based on the laws and regulations relevant to information security, including the Clinger-Cohen Act of 1996, the Federal Information Security Management Act (FISMA) of 2002, and Office of Management and Budget (OMB) Circular A-130. The material in this handbook can be referenced for general information on a particular topic or can be used in the decision-making process for developing an information security program.

Status: Completed
Controlling Organization: National Institute of Standards and Technology
Contact Information:
Public Inquiries Unit
NIST, 100 Bureau Drive, Stop 1070, Gaithersburg, MD 20899-1070
Email: inquiries@nist.gov
Phone: (301) 975-NIST (6478) or TTY (301) 975-8295
URL: http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf

## 1.4. COMMON FRAMEWORKS BETWEEN FINANCIAL SERVICES AND INSURANCE INDUSTRY

### 1.4.1. CONTROL OBJECTIVES FOR INFORMATION TECHNOLOGY (COBIT®)

**Description**: Control Objectives for Information and related Technology (COBIT®) provides good practices across a domain and process framework and presents activities in a manageable and logical structure. COBIT's good practices represent the consensus of experts. They are strongly focused more on control, less on execution. These practices will help optimize IT-enabled investments, ensure service delivery and provide a measure against which to judge when things do go wrong.

Status: Complete
Controlling Organization: The Information Systems Audit and Control Association (ISACA)
Contact Information: http://www.isaca.org
URL: www.isaca.org/cobit.htm

### 1.4.2. ENTERPRISE RISK MANAGEMENT - COSO

**Description:** COSO ERM describes risk management as "a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."

Status: Complete
Controlling Organization: Committee of Sponsoring Organizations of the Treadway Commission
Contact Information: http://www.coso.org
URL: http://www.coso.org/publications.htm

### 1.4.3. INFORMATION SECURITY MANAGEMENT MATURITY MODEL (ISM3)

**Description**: The Information Security Management Maturity Model (ISM3, or ISM-cubed) extends ISO9001 quality management principles to information security management (ISM) systems. Rather than focusing on controls, it focuses on the common processes of information security, which are shared to some extent by all organizations.

Under ISM3, the common processes of information security are formally described, given performance targets and metrics, and used to build a quality assured process framework. Performance targets are unique to each implementation and depend upon business requirements and resources available. Altogether, the performance targets for security become the Information Security Policy. The emphasis on the practical and the measurable is what makes ISM3 unusual, and the approach ensures that ISM systems adapt without re-engineering in the face of changes to technology and risk.

Implementations of ISM3 are compatible with ISO27001 (Information Security Management Systems – Requirements), which establishes control objectives for each process. Implementations use management responsibilities framework akin to the IT Governance Institute's CobIT® framework model, which describes best practice in

the parent field of IT service management. ITIL users can employ ISM3 process orientation to strengthen ITIL security process seamlessly. Using ISM3 style metrics, objectives and targets it is possible to create measurable Service Level Agreements for outsourced security processes.

Status: Complete
Controlling Organization: ISM3 Consortium
Contact Information: consortium@ism3.com
URL: http://www.ism3.com

### 1.4.4. FACTOR ANALYSIS OF INFORMATION RISK (FAIR)

**Description: The FAIR Risk Management Framework. Factor Analysis of Information Risk (FAIR) provides a framework for understanding, analyzing, and measuring information risk. The outcomes are more cost-effective information risk management, greater credibility for the information security profession, and a foundation from which to develop a scientific approach to information risk management.**

Status: Complete
Controlling Organization: Risk Management Insight
Contact Information:
Risk Management Insight
T (614) 441-9601 F 1 (815) 377-1163
URL: info@riskmanagementinsight.com
http://www.riskmanagementinsight.com
http://fairwiki.riskmanagementinsight.com/
http://www.riskmanagementinsight.com/media/docs/FAIR_introduction.pdf

### 1.4.5. OPERATIONALLY CRITICAL THREAT, ASSET, AND VULNERABILITY EVALUATION (OCTAVE)

**Description**: This document describes the Operationally Critical Threat, Asset, and Vulnerability Evaluation SM (OCTAVE®), an approach for managing information security risks. It presents an overview of the OCTAVE approach and briefly describes two OCTAVE-consistent methods developed at the Software Engineering Institute (SEI).

The overall approach embodied in OCTAVE is described first, followed by a general description of the two methods: the OCTAVE

Method for large organizations and OCTAVE-S1 for small organizations. Information is provided to assist the reader in differentiating between the two methods, including characteristics defining the target organization for each method as well as any constraints and limitations of each method. OCTAVE will be replaced by the Carnegie Mellon University Software Engineering Institute Resiliency Framework in the near future. The Resiliency Framework's scope is broader then OCTAVE and will cover a variety of aspects of security for the financial services industry. The Resiliency Framework provides a good overall resource for managing risks within a complex modern organization.

Status: Complete
Controlling Organization: CERT
Contact Information: http://www.cert.org/
URL: http://www.cert.org/octave/

### 1.4.6. COMMON VULNERABILITY SCORING SYSTEM (CVSS V.2)

**Description**: The Common Vulnerability Scoring System (CVSS) provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. CVSS consists of three groups: Base, Temporal and Environmental. Each group produces a numeric score ranging from 0 to 10, and a Vector, a compressed textual representation that reflects the values used to derive the score. The Base group represents the intrinsic qualities of a vulnerability. The Temporal group reflects the characteristics of a vulnerability that change over time. The Environmental group represents the characteristics of a vulnerability that are unique to any user's environment. CVSS enables IT managers, vulnerability bulletin providers, security vendors, application vendors and researchers to all benefit by adopting this common language of scoring IT vulnerabilities.

Status: Complete
Controlling Organization: Forum for Incident Response and Security Teams
Contact Information: Secretariat can be contacted at first-sec at first.org

URL: http://www.first.org
URL: http://www.first.org/cvss/cvss-guide.html

## 1.5. COMPARISON OF STANDARDS ACROSS INDUSTRIES

A comparison of the standards found in the financial services and insurance industries reveals the following gaps and overlaps. The following table includes the specific frameworks reviewed by the study group and reflects the study group membership's observations of the level of adoption of each framework in their institutions or by peers. Frameworks that were not formally published at the time of this report were identified as "Under development" to indicate their adoption was not practically possible. The items identified as "In wide use" had multiple institutions either currently using the standard or in the process of adopting the standard. The items identified as "In limited use" were recognized as being used in only a few institutions or as being considered for future adoption. The items identified as "Not in use" were not recognized by working group members as not being adopted in their institutions nor in peer organizations. The reasons for this varied, in some cases due to an apparent lack of direct knowledge of the specific standard, or in other cases (such as the NIST 800 frameworks) the standards noted are well known, but not generally adopted in either Financial Services or the Insurance Industry, most likely due to their primary focus on some other sector, such as government.

Table 1. STANDARDS AND REFERENCE DOCUMENTS USED IN FINANCIAL SERVICES AND INSURANCE SECURITY OPERATIONS

| Standard \| Reference Work Title | Financial Services | Insurance |
|---|---|---|
| ISO/IEC 27001:2005, Information technology - Security techniques - Information security management systems - Requirements | In wide use/ Complete | In wide use/ Complete |
| ISO/IEC 27002:2005, Information technology -- Security techniques -- Code of practice for information security management | In wide use/ Complete | In wide use/ Complete |

| | | |
|---|---|---|
| ISO/IEC 2nd FCD 27004, Information Security Management Measurement | Under Development | Under Development |
| ISO/IEC 2nd FCD 27005, Information technology -- Security techniques -- Information security risk management | Under Development | Under Development |
| ISO/IEC FDIS 21827 -- Information technology -- Security techniques – Systems security engineering – Capability maturity model (SSE-CMM®) to Address Cyber Threats | Not in use/ Complete | Not in use/ Complete |
| NIST 800-53 - Recommended Security Controls For Federal Information Systems | Not in use/ Complete | Not in use/ Complete |
| NIST 800-30 - Risk Management Guide For Information Technology Systems | Limited use/ Complete | Not in use/ Complete |
| NIST 800-55r1 - Performance Measurement Guide For Information Security | Under Development | Under Development |
| NIST SP 800-100 - Information Security Handbook – A Guide For Managers | Not in use/ Complete | Not in use/ Complete |
| Control Objectives for Information Technology (CobiT®) | In wide use/ Complete | In wide use/ Complete |
| Enterprise Risk Management - COSO | Limited use/ Complete | Not in use/ Complete |
| OCTAVE Allegro: Improving the Information Security Risk Assessment Process | Limited use/ Complete | Limited use/ Complete |
| FFIEC IT Examination Handbook | In use/ Complete | Not in use/ Complete |
| Security Operations Maturity Architecture (SOMA) | Limited use/ Complete | Limited use/ Complete |
| Information Security Management Maturity Model (ISM3) | Limited use/ Complete | Limited use/ Complete |
| An Introduction to Factor Analysis of Information Risk (FAIR) | Limited use/ Complete | Not in use/ Complete |

# 2. Findings and Recommendations

## 2.1. FINDINGS

### 2.1.1. USABILITY OF STANDARDS BY THIRD PARTIES:

Third party providers, such as outsource vendors or contract labor providers, need a better way to interpret or translate the various terms and techniques used in the portfolio of standards and frameworks applicable to different industries and organizations. This is needed to help them determine the level of interoperability and estimate the level compliance of that could be expected from different solutions. This may be provided by a supporting document or an awareness campaign rather than new (or revised) standards. In addition to the taxonomy, it would be beneficial to have a cross-walk or mapping of the security controls of various standards, regulations and other mandatory guidance. This document would provide guidance on how to reconcile the controls and processes necessary to meet the requirements of existing security standards against any similar controls or processes used to meet the requirements of other standards and regulations, be they industry, national or international in origin. Additionally, the linkage between compliance frameworks, risk models, and maturity models should be improved so they work in conjunction with each other without leaving the end user to create their own set of mapping criteria.

### 2.1.2. CONNECTING DISPARATE EFFORTS OF STANDARDS COMMITTEES AND OTHER INDUSTRY AND GOVERNMENT ENTITIES THAT MAY NOT VISIBLE TO THE FS AND INSURANCE INDUSTRY:

Standards work is done in vertical committees where collaboration is dependent on the liaisons established by these committees. As a general observation there is a lot more intersections in the work then committees may realize at any given point in time. As a part of a suggested awareness campaign, efforts by other standards groups and industry groups could be highlighted to increase awareness of future standards and tools that could help solve the current challenges. For example, SC7 is in the process of developing a draft ISO/IEC 15026, System and Software Assurance which aims at helping the buyers of software assure that software vulnerabilities have been minimized throughout the development process. Another example is a number of efforts headed by NIST and DHS to

create and make available to the industry enumerations of vulnerabilities, weaknesses, etc. to enable interoperability of vendor tools to identify and manage potential vulnerabilities on software and systems. The most famous is the National Vulnerability Database (NVD). Use of such tools will help quantify the risks and measure current and potential exposure. Industry could participate as a member of working groups that provide inputs into these efforts and get up to speed on what is happening. The NVD uses the Common Vulnerability Scoring System (version 2) to rate the impact severity of vulnerabilities along the three dimensions of Confidentiality, Integrity, and Availability. It produces a numerical weighting as a base score and that can be modified with environmental and temporal scores based upon the institutions environment and the current state of corrective actions available.

### 2.1.3. USAGE BY TECHNOLOGY PROVIDERS:

Many technology providers will supply only a component element of the larger solution so interoperability between these various components will be key to adoption. Defining a core, or base of technology interfaces that is extensible to address the varying needs of the typical enterprise should be a principal consideration for the group. It is also important that we consider the current trends in the software and services delivery model as it relates to the use of Software as a Service and Application Service Providers wherein the vendor community is taking some responsibility / liability for the compliance processes and changing the risk profile dramatically.

### 2.1.4. RISK WEIGHTING CONTROL FRAMEWORKS

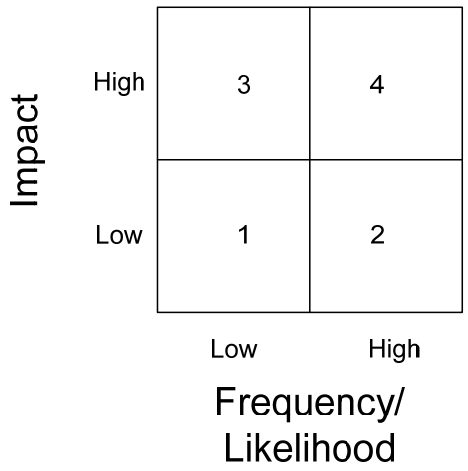
Adjusting control requirements based upon outcomes of risk assessments can be a way of making control frameworks much more efficient and responsive to real-world business situations. This can also greatly benefit from integration with the vulnerability impact assessment schemes such as CVSS. (This was seen as a positive emerging trend in both the NIST 800-x and ISO/IEC 27xxx series with work in progress from both groups.) More study and

development around categorization\ measurement of threat is needed as input to the risk models. The basic calculus of risk seems to be converging on a formula where Risk is the product of (Threat x Vulnerability x Likelihood x Asset Value). None of the standards texts presumes to compute asset value and only CVSS attempts to measure vulnerability. CVSS seems to have the widest adoption as a vulnerability scaling/scoring methodology and is best suited to technical vulnerabilities. Non technical vulnerabilities lack a measurement methodology that would need to be addressed. Asset value measurement methods vary greatly by institution, but are generally well enough understood to be the most productive area to begin developing supporting standards.

### 2.1.5. HANDLING OF HIGH IMPACT, LOW PROBABILITY EVENTS:

The area that causes the most inconsistency due to the inherent complexity of assessment and the operating modes of the risk assessment models is with the "High Impact, Low Likelihood" events (quadrant 3, below). The other 3 quadrants of the chart below are handled by the risk management models available within the limitations noted elsewhere in this report. Direct impacts, such as losses, are reasonably well handled in the all models while "brand" or "franchise" impacts are still highly subjective. High Likelihood\Frequency events are also reasonably well addressed as there are some quantitative or qualitative measurements and data for coarse grain segmentation.

Figure 1. Risk Impact vs. Frequency Matrix




Quadrant 1 would have minimal to no control requirements. Quadrant 2 would be addressed by minimal controls as defined in the control frameworks when integrated with the risk assessment. Quadrant 4 risks would be handled by the maximal controls from the framework. As Quadrant 3 is highly variable, the risk models would have to be enhanced to increase their sensitivity to High Impact, Low Frequency events as this is the most significant variance in output in risk assessment results.

## 2.2. GENERAL RECOMMENDATIONS

Members of the Study Group contributed perspectives and best practices to the report, which apply generally to its recommendations. These contributions are summarized in this section.

### 2.2.1. BUSINESS (OR ORGANIZATIONAL) VALUE:

FS and Insurance industries are under heavy pressure to comply with multiple regulatory requirements that are either very general or very specific. Regulation in the US normally does not reference specific standards and is aimed at a final result/behavior by industry. Standards exist to address risk management and compliance concerns but none provide a full comprehensive solution. However,

integration of several relevant standards into a framework can provide a comprehensive risk management and compliance solution that will facilitate proactive management of future risks and regulatory compliance concerns. Additionally, tools and techniques identified in the standards need to state results that more easily map to tangible impacts to the bottom line (e.g., business value) can be recognized by organizational management. FS and Insurance industry executives may or may not be aware of the value of standards, such as ISO/IEC 27001, for demonstrating regulatory compliance because the legislation in question does not reference specific standards. Rather than developing specific new standards that are likely to meet a similar fate, three solutions could be helpful:

- An awareness campaign by INCITS could expand the support base and use of already existing standards to help Financial Services and Insurance industry demonstrate compliance with current and emerging legislation and regulation. Outreach to regulatory bodies to consider external frameworks for adoption/inclusion into rule making or examination procedures could accelerate this process.
- A guidance document that clearly communicates that the application of multiple integrated standards beyond the basic checklist mentality of applying controls could be beneficial to both suppliers and clients, such as a guidance document that illustrates how ISO/IEC 27001 and ISO/IEC 20000 interact and support one another. This guidance document would illustrate the synergy between the standards and stress the importance of the risk management process in selecting which controls are applied, and to what level. Addressing this 'gap' in understanding would provide a basis for industries, suppliers and vendors to more consistently discuss the application and adoption of security standards.
- Requesting that INCITS committees harmonize relevant standards and work with the respective ISO committees to

do so. It should be noted that there is an ongoing effort by ISO to harmonize and integrate all management system standards including ISO 9000, ISO 14000, ISO/IEC 20000, ISO/IEC 27001, and potentially others. A harmonized US position that supports this ISO direction could help in the long term. As management system standards come up for revision, such as ISO/IEC 27001 and 27002, it may be appropriate to look for opportunities to accomplish such harmonization or to integrate additional controls into their respective control catalogues that address these concerns.

### 2.2.2. INFORMATION SECURITY MEASURES AND MEASUREMENTS

A current weakness in the guidance provided by standards and available to all industries, including Financial Services and Insurance, is the lack of common measures and measurements. Such standards are necessary to provide a common language for identifying, characterizing, valuing and communicating information related to risks, vulnerabilities, control effectiveness, weaknesses and areas of improvement with stakeholders and others involved in information security management. The following actions and activities are recommended:

- INCITS should continue to encourage members and other interested parties within their span of influence to actively participate in and support the current efforts to develop ISO/IEC 27004. This activity should include, and may be led by, members of the SG-SBP
- A new study group should be formed with a charter to gather existing practices, procedures, measures and measurement techniques related to information security, identify specific areas of existing commonality or opportunity, and provide recommendations to include in ISO/IEC 27004 and other standards as best practices

- INCITS should also determine if there are any identified areas of concern with the draft ISO/IEC 27004 standard that could affect support for an affirmative vote and charter individuals or a formal working group to identify possible resolution paths for each.

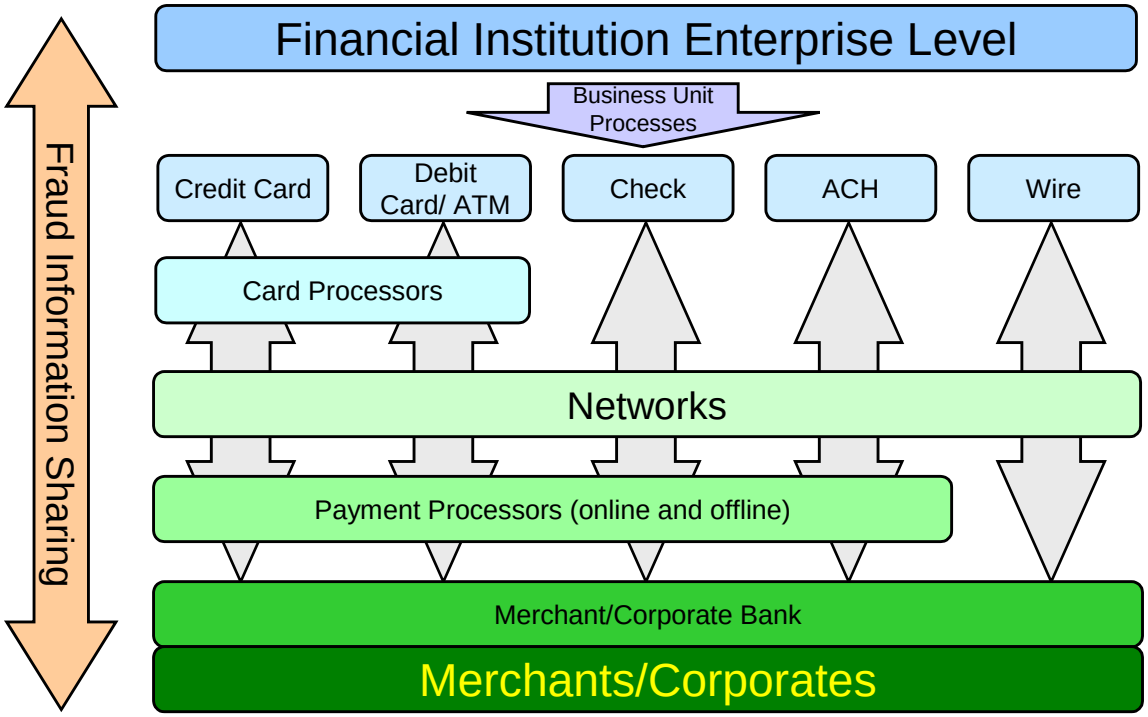
## 2.3. RECOMMENDATION FOR RISK WEIGHTING CONTROL FRAMEWORKS

In order to better foster adoptability of the control frameworks (ISO 27xxx, NIST, etc) they need to be optimized to define control requirement requisite to the risks of the assets or organization. The risk assessment methodology output needs to be directly tied to the application of control requirement statements. The expectation would be that greater/stronger controls are mandated for items with higher risk and lesser controls for items with lower risk. Additionally, the output of the risk assessment also needs to offer implementation guidance for how different models address the selection of appropriate controls for "High Impact, Low Probability" events. This was noted as the area that most significantly impacts the adoptability of the frameworks. To a limited extent, this expectation is addressed by some of the frameworks, but the working group believes this area needs to be greatly enhanced.

## 2.4. DEVELOPMENT OF INFORMATION SHARING TO BE USED AS INPUT TO RISK MODEL

While it is important for financial institutions and insurance companies to maintain security standards within their own facilities, the possibilities for cooperation, particularly with non-financial firms such as merchants or corporations, should not be ignored. Particularly in areas such as payments or securities transactions, financial institutions see only a part of the transaction, and must rely on payment processors, merchants, consumers and other financial institutions to complete the picture, as shown in Figure 2.

**Figure 2. Payments Participants across Transaction Types**




One possible output for such collaboration would be the development of a cross-industry or an industry-specific fraud database, collecting information at a high level from all stakeholders in the system, from financial institutions to customers. Information held in the database could be used by financial institutions to evaluate the success of their security measures, or to aid in building stronger fraud detection models. While the example given in Figure 1 is specific to the payments industry, a similar approach could be used for the capital markets or insurance industry.

- The study group recommends that financial services firms and associations look for ways to build collaborative databases that can be used to improve risk management across respective industries in a manner similar to that illustrated above.

# 3. The Study Group on Security Best Practices (SG-SBP)

## 3.1. TERMS OF REFERENCE AS SPECIFIED BY THE INCITS EXECUTIVE BOARD

The INCITS Study Group on Security Best Practices will:

- Study the security needs and requirements of the financial and insurance services industries and assess what is missing in current standards and practices.
- Make a recommendation to the INCITS EB on an approach to create deployable best practices and frameworks for security in these industries. This may include creating Project Proposals for new INCITS Standards or Technical Reports.
- Complete its work and submit its report for consideration at the January 2008 INCITS EB meeting.

## 3.2. Challenges

Given the intended short lifecycle of the SG-SBP, getting information to the two very large industry sectors of financial services and insurance is paramount but difficult. Nonetheless, this has happened, particularly with the help of press releases and the FST Summit (Financial Services Technology Summit) conference held in Scottsdale, Az., in September 2007. Similarly, getting to the appropriate influential organizations and individuals as well as those with the appropriate expertise was yet another challenge which was met through strategic relationships with key standards organizations and industry consortia.

## 3.3. Formal Meetings

| 2007 – 2008 Previous Meetings | | |
|---|---|---|
| Meeting | Dates | Location |
| 1 | Sep 19 | Scottsdale, Az. |
| 2 | Oct 4 | (telecon) |
| 3 | Oct 12 | (telecon) |
| 4 | Oct 23 | (telecon) |
| 5 | Nov 20 | (telecon) |
| 6 | Dec 10 | (telecon) |
| 7 | Dec 18 | (telecon) |
| 8 | Jan 7 | (telecon) |

## 3.4. Liaisons and External Contacts

The Study Group determined that the most effective means for reaching consensus in the Financial Services and Insurance industries is through collaboration and liaison with other Standard Development Organizations and industry organizations. This approach has a number of benefits, but the most significant is simply a greater enabled outreach and secondly to take advantage of the pervasive influence and knowledge available in such organizations.

Below are two major categories for industry organizations, including major standards organizations and industry consortia: The first category is the organizations which the Study Group has contacted and the second are additional organizations which should be contacted as the recommendations of this report are pursued.

| Organization contacted | |
|---|---|
| **Organization** | **Contact** |
| BITS (www.bitsinfo.org) | Ann Patterson<br>Vice President, Relationship Management<br>T 202-589-2448<br>F 202-628-2492<br>ann@fsround.org |
| DHS – Department of Homeland Security | Peter Shebell<br>Standards Policy Manager<br>Department of Homeland Security<br>Science & Technology Directorate<br>Test & Evaluation and Standards Division<br>202-254-5706 (voice)<br>peter.shebell@dhs.gov (e-mail)<br>202-680-3449 (cell) |
| FSTC – Financial Services Technology Consortium ( www.fstc.org) | John Fricke<br>Chief of Staff, VP<br>O: 281-692-0011<br>john.fricke@fstc.org |
| INCITS CS1- Cyber Security | (see NIST below) |
| INCITS CT 22 | James W. Moore, CSDP, F-IEEE<br>The MITRE Corporation<br>7515 Colshire Drive, H505,<br>McLean, VA 22102-7508<br>Office: +1.703.983.7396 Fax: +1.703.983.1279<br>Cell: +1.301.938.0260<br>Email for MITRE use: moorej@mitre.org. |

| Organization contacted (continued) | |
|---|---|
| **Organization** | **Contact** |
| INCITS T3 – Open Distributed Processing | Edward L. Stull,<br>T3, Chair<br>20600 Georgia Avenue,<br>Brookeville, MD 20833<br>301 260-1781<br>edstull@elstull.com |
| NIST – National Institute of Standards and Technology | Daniel R. Benigni, Chair<br>INCITS CS1, Cyber Security<br>US TAG for ISO/IEC JTC 1/SC 27<br>and all SC 27 Working Groups<br>National Institute of Standards & Technology<br>Information Technology Laboratory<br>Computer Security Division<br>System and Network Security Group (893.02)<br>100 Bureau Drive, Mail Stop 8930<br>Gaithersburg, MD 20899-8930<br>Phone: 301-975-3279<br>Fax: 301-975-8387<br>Email: dbenigni@nist.gov |
| X9 - Accredited Standards Committee (ASC) X9, Financial Services | Cindy Fuller<br>ASC X9, Inc.<br>1212 West Street, Suite 200<br>Annapolis, Maryland 21401<br>Telephone: (410) 267-7707<br>Fax: (410) 267-0961<br>Email: cindy.fuller@X9.org |

| Organizations to be contacted in the future |
|---|
| AHIP - America's Health Insurance Plans |
| DOD – Department of Defense |
| JTC1 SC27 - IT Security techniques |
| LOMA (although initially contacted through a member of the Study Group, Micki Krause, no further action was taken) |

## 3.5. OFFICERS

| POSITION | NAME | ORGANIZATION |
|---|---|---|
| Chair | Edward L. Stull | Direct Computer Resources, Inc. |
| Vice Chair, Financial Services | Mark G. Clancy | Citigroup, Inc. |
| Vice Chair, Insurance | Robert E. Talbot | Coventry Health Care, Inc. |
| Secretary | Nadya Bartol | Booz Allen & Hamilton Inc |

## 3.6. **MEMBERSHIP**

BITS (Liaison)
- Ann Patterson

Booz Allen & Hamilton Inc (Voting)
- Mike Gerdes
- Nadya Bartol

Citigroup, Inc. (Voting)
- Mark Clancy
- Richard Gomes

Communication Intelligence Corporation (Advisory)
- Russ Davis

Coventry Health Care, Inc. (Voting)
- Robert Talbot
- Tom Wehrle

Credit Industriel et Commercial (Voting)
- Jean-Pierre Champigny
- Ken Belva

Department of Homeland Security (Liaison)
- Peter Shebell

Direct Computer Resources, Inc. (Voting)
- Joe Buonomo
- Ed Stull

Financial Insights (Voting)
- Aaron McPherson

Financial Services Technology Consortium (FSTC) (Liaison)
- John Fricke

IBM Corporation (Voting)
- Christine Knibloe

INCITS CS1 - Cyber Security (Liaison)
- Dan Benigni

INCITS CT 22 (Liaison)
- James W. Moore

INCITS T3 (Liaison)
- Ed Stull

National Institute of Standards and Technology (Liaison)
Dan Benigni
Orange Parachute (Voting)
Kim Sassaman
X9, Inc.
Cindy Fuller
Zions Bancorporation (Voting)
Preston Wood

## 3.7. Appreciation

The membership of the SG-SBP recognizes the vision of Karen Higginbottom, Scott Jameson and Edward Barrett in conceiving the mission for the Study Group and is most grateful for the opportunity and support given it by the INCITS Executive Board and its members.

The SG-SBP further recognizes the extraordinary support of the INCITS Secretariat, in particular Jennifer Garner Deborah Spittle and Lynn Bara, for the critical assistance needed to launch and support the study group.