BITS
FINANCIAL SERVICES ROUNDTABLE

The Innovator

This Issue: A Discussion of the Role of Standards in the Financial Services Industry

In This Issue:

We value your opinion. Please contact Dan Schutzer, Dan@fsround.org if you have comments about this edition of *The Innovator*.

Disclaimer: The views and opinions expressed in the enclosed articles are those of the authors and do not necessarily reflect the official policy or position of The Financial Services Roundtable or BITS.

BITS and BYTES: The Importance of Standards to the Financial Services Industry

By Dan Schutzer, BITS

Standards play an important role in the evolution of technology advances and in their ultimate success and integration into society and business. Standards can serve many needs including:

1. Ensure interoperability between various diverse, independently developed products and services
2. Support competition by enabling products from multiple competitors to work together, preventing vendor lock-in
3. Make it easier for a new technology to reach critical mass by allowing users of different vendor products to interact with each other
4. Support innovation by making it easier for new products to be built on top of existing infrastructure
5. Ensure a minimum standard of prudence and level of performance is achieved.

When a new technology is first invented, there is a period of exploration and competition. At this point there is little incentive for the technology innovators to cooperate in specifying and complying with a standard as they are still learning how the technology will be used and what features and functions are important. Furthermore, everyone is hoping to achieve a dominant position, and is not interested in making it easier for their competitors to interoperate with their products.

Standards typically can evolve out of two broad scenarios. The first scenario occurs when the work of a single vendor (or vendor consortium, that is, a small group of collaborative vendors) succeeds in developing a product that so dominates in the marketplace that it becomes essential for others to interface with it on the vendor's terms. The vendor, or vendor consortium, then publishes standards necessary to interface with their product and these standards become a de facto standard by virtue of their broad acceptance in the marketplace.

The second scenario occurs in situations where no single vendor or vendor consortium has achieved total dominance. As the technology advance matures and begins to enter mainstream adoption, everyone becomes more motivated to establish open, consensus-driven standards.

Today, standards important to the financial services industry are being developed and maintained by a number of standards bodies, some ad hoc, some consensus-based, and some managed by an official accredited standards body.

In this issue we hear from some of these standards-setting bodies about current standards activities that are likely to be of interest to the financial services industry, including:

- Accredited Standards Committee X9 (ASC X9), who is accredited by American National Standards Institute (ANSI), and also acts as the secretariat for International Organization for Standardization Technical Committee 68 (ISO TC 68), who is working on standards in the areas of payments, securities and related security technologies;
- North American Security Standards Productions Organization (NASPO), also accredited by ANSI, about work they are doing in the areas of identity proofing and verification and fraud countermeasures;

- Payment Card Information (PCI) Security Standards Council about their work on setting security standards to secure card-related data;
- The Santa Fe Group about the Shared Assessments Program which provides standards and tools for assessing IT outsource vendors; and
- World Wide Web Consortium (W3C) about their standards activities in Web technologies, with emphasis on the emerging semantic web.

In addition, Michael Sukkarieh of Citigroup provides his view of the role of standards in assessing security and privacy and Rama Moorthy and Mike Oara of Hatha Systems discuss standards emerging in the area of analyzing and understanding application software and their usefulness in a number of areas including performing security and vulnerability assessments and migration planning.

These papers are not intended to provide a complete list of standards bodies and standards under development that are relevant to the financial services industry, but rather to provide a sampling that can offer better insight into the role standards play in the financial services industry. Please contact me at Dan@fsround.org if you are interested in learning more about the standards activities discussed here or about other ongoing standards activities.

Thanks and happy reading.

NASPO and the Identity Proof and Verification Project

By Graham Whitehead, NASPO

About NASPO[1]

NASPO is the North American Security Products Organization. NASPO is focused on the development of standards that counter and control product related, identity and document related financial fraud. Founded in 2002, in Washington DC, NASPO is a non profit organization that was accredited by the American National Standards Institute (ANSI) in 2004 as an American National Standards Development Organization (SDO). In 2009, NASPO instigated and together with ANSI created the ISO Fraud Countermeasures and Controls Committee – ISO TC247. On behalf of ANSI and the USA, NASPO now serves as secretariat and chair of the ISO Technical Committee on Fraud Countermeasures and Controls – ISO TC 247 and the US TAG that supports it.

Programs and Projects

Standards Development – NASPO is currently responsible for the development of :

i. An American National Standard (ANS) for proof and verification of personal identity. This project is on-going and known as the NASPO IDPV Project.
ii. An international, ISO Security Risk Management System Standard – ISO 16125.

Standards Administration – As an ANS-SDO, NASPO is responsible for initiation of ANS projects, funding them, providing secretariat services and fostering their operation in accordance with the essential requirements of ANSI[2]. On behalf of ANSI and the USA, NASPO is responsible for management and administration of the ISO Fraud Countermeasures and Controls Committee – ISO TC247 and associated US Technical Advisory Group.

Standards Maintenance – NASPO is responsible for periodic maintenance of the American National Security Assurance standard, ANSI/NASPO-SA-2008. An open invitation to participate in a review and update of this standard was be published by ANSI and NASPO on June 1, 2011.

Certification - In 2005, NASPO created the American National Security Assurance Standard[3] and updated it in 2008 as ANSI/NASPO-SA-2008. This standard is applicable to any organization that is required by virtue of the nature of its products and services to demonstrate a moderate, high or very high level of resistance to all common and unique security threats. Certification of compliance with this standard is a major program of work for NASPO. This work is carried out by auditors selected and trained by NASPO under the direction of the NASPO Director of Auditing. Organizations certified by NASPO as being in compliance with one of 3 levels of threat resistance specified in ANSI/NASPO-SA-2008 are identified on the NASPO website, http://www.naspo.info/.

Accreditation – NASPO accredits commercial certification bodies to certify compliance with standards for which NASPO is the standard authority. To date, TUV Rheinland has been accredited by NASPO to certify compliance with the American National Security Assurance Standard, ANSI/NASPO-SA-2008. Other commercial certification bodies are currently being accredited.

---

[1] For more information about NASPO go to: NASPO

[2] ANSI Essential Requirements: Due process requirements for American National Standards (2008 Edition). This document is available at : ANSI Due Process Requirements.

[3] The ANSI/NASPO Security Assurance Standard, ANSI/NASPO-SA-2008 is available for purchase from the NASPO Web Store.

These accreditations are expected to further expand international demand for certification to this ANS.

Vocational Training and Professional Development – Aimed at security managers and teams, the training provided by NASPO is delivered in regular quarterly workshops and dedicated site visits. The training workshops impart a detailed understanding of the requirements of the security assurance standard and implementation guidelines. A professional development program is imminent. This program will offer and provide professional qualifications in security risk management.

The NASPO Identity Proof and Verification Project (IDPV)

It was the IDPV that brought NASPO into contact with BITS. The IDPV project is an outgrowth of the ANSI Identity Theft and Identity Management Standards Panel (IDSP)[4] and subsequent work performed under the auspices of NASPO that culminated in an ANSI report[5] and NASPO report[6]. The ANSI report identified the need for development of a national identity proof and verification standard. The NASPO report provides an account of the subsequent NASPO ID-V effort made to formulate viable solution concepts for problems annunciated by the ANSI report. The NASPO ID-V report, and lessons learned from that work, established the starting point for the NASPO IDPV project. At a kick off meeting[7] in July 2010, a body of experts and interested parties[8] was formed by NASPO to reach consensus on the national standard. The scope of the IDPV project was established by the IDPV consensus body as follows:

> *The development of an American national standard and implementation guidelines for identity proofing processes, verification processes and requirements for information to be used in support of identity establishment for end users and relying parties.*

Today, in the US, it is easy to make yourself into someone else if you have an incentive - plenty do! - as evidenced by the incidence of identity theft. Being an imposter is made particularly easy in the US by the existence of what are termed "open record" states. In these states, anyone can obtain a copy of another person's birth certificate. Some read the obituary pages and trade on the frequent time delay in registration of the deceased. The "acquired" birth certificate, together with other fake and insecure documents are then used to "breed" photo identity documents (such as a state-issued driving license or identity card and from that a passport[9]) that are generally accepted as proof that you are who you claim to be. The issue of "open record" states would, of course, be acceptable, if the record of birth was incontrovertibly linked to the person who claims to own it – it is not! The link (some form of unique biometric identifier) is missing. Hence, there is no way, at this time to know if an identity asserted by presentation of a birth certificate is true or false. To make matters worse becoming, working and living life as an imposter is also made easy by:

- a substantial lack of concern by citizens about their identity credentials getting into the wrong hands
- the power of internet search engines that enable an imposter to know details of a victims life history

[4] For more information on the ANSI IDSP go to: ANSI IDSP
[5] The ANSI report is available for free download at IDSP Workshop Report
[6] The NASPO ID-V Project report is available for free download at NASPO ID-V Project Report
[7] Reports of IDPV meetings are openly available at: NASPO IDPV Meeting Reports
[8] BITS is a participating member of the IDPV consensus body
[9] An example of birth certificates obtained and used in this way is given in GAO Report GAO-09-447: DEPARTMENT OF STATE Undercover Tests Reveal Significant Vulnerabilities in State's Passport Issuance Process. This report is available at GAO-09-447

- the lack of a solid identity reference system and access to identity related data bases
- the ease with which certain documents used as proof of identity can be altered or fabricated.

Financial institutions are well aware that the most insidious exploiters are those who use their true identity for official purposes and multiple false identities to commit identity related financial fraud. Consistent with it's approach to the development of other standards, NASPO is taking a top down, risk management, overall systems approach to the development of the IDPV standard. This approach is taking into consideration:

- the needs of relying parties (RPs)[10]
- the needs of Identity Providers (IDPs)
- the need for RPs to know how and with what certainty an IDP has removed suspicion of specific types and techniques of identity fraud of concern to the RP
- the need of both RPs and IDPs to know that the proof and verification processes do not violate the The Fair Information Practice Principles (FIPPs) (see PRIVACY POLICY GUIDANCE MEMORANDUM, Memorandum number 2008-1. December 29, 2008)
- the need to establish a solid and verifiable chain of identity trust.

To these ends, the IDPV standard is expected to place mandatory requirements on:

A. Relying Parties (RPs)
   - to perform an assessment of the impact of accepting a false assertion of identity
   - to specify types and techniques of identity fraud that must be detected by an IDP including any not listed in the standard that are known to be unique to a specific RP
   - to specify the techniques to be used by an IDP to detect each type and technique of identity fraud of concern to an RP for persons asserting US citizenship and a foreign birth place
   - to specify the detection criteria to be used by an IDP to establish that a symptom of fraud has been detected
   - to work cooperatively with an IDP to establish the weight of impact to be assigned to contra indications that result from detection of fraud symptoms
   - to specify criteria for acceptance/rejection of an asserted identity
   - to obtain evidence that the IDP is in compliance with the IDPV standard.

B. Identity Providers (IDPs)
   - to remove suspicion of all types and techniques of identity fraud specified by an RP
   - to use methods of detection of types and techniques of identity fraud specified by the standard
   - to use modes of interaction (such as in-person, remote assisted, remote unassisted) with the person specified by the standard
   - to use fraud detection criteria specified by the standard and approved by the RP
   - to compile results in the form of a contra-indications table that can be shared with the RP
   - to weight findings of fraud in accordance with those specified by the standard and approved by the RP

[10] The terminology used in the IDPV standard will be consistent that used in the National Strategy for Trusted Identities in Cyberspace (NSTIC)

- to use the criteria specified by the standard and approved by the RP for acceptance or rejection of an asserted identity.
- to provide RPs with evidence of compliance with the IDPV standard.

The standard is expected to address all known types and techniques of identity fraud including document fraud, record or IDP insider fraud and imposter fraud. It will also require an RP to identify and treat types and techniques of identity fraud that are unique to the RP and not addressed by the standard. The standard will be updated, with the issuance of "New Fraud" Bulletins in the event that new types and techniques of identity fraud emerge.

The detection techniques specified in the IDPV standard (that are critical to the efficacy and viability of the IDPV standard) are expected to be based on an identification of the symptoms that uniquely identify each type and technique of fraud. The techniques are expected to include: document authentication, personal interaction, data base cross referencing and internal IDP audits.

In response to the "Know Your Customer" demands of the Patriot and other Acts and to protect themselves from rampant imposter fraud, financial institutions have been making increasing use of dynamic knowledge-based authentication technology. By combining, in the IDPV standard, the power of this technology with document authentication technology, identity data base cross referencing, and binding to a biometric attribute, users of the standard will be able to detect and control many types and techniques of identity fraud that are currently under the radar.

X9 Leads Industry Resurgence: New Role for Financial Industry Standards

By Cindy Fuller, ASC X9

The modern era for banking and financial industry standards began shortly after World War II when financial institutions began the "electronification" of paper checks, and new messaging practices. From here, standards rapidly moved to other business and process standards, including electronic payments, credit/debit card transactions, electronic data security and messaging. Actually, the role for standardization of new financial services technology has never stopped.

Today, the Accredited Standards Committee X9 (X9 or ASCX9) has become the primary standards development organization for the financial services industry. X9 is the sole financial industry standards body accredited by both the American National Standards Institute (ANSI) and as the US TAG to the International Standards Organizations (ISO) Technical Committee 68 (TC 68). TC 68 holds the US vote for the approval of ISO financial services/banking standards and further acts as the committee Secretariat.

It is important to know that neither ANSI nor ISO create standards. Both ANSI and ISO are independent organizations who oversee the rules and processes for development of technical standards prepared by national standards bodies for accreditation and implementation. ANSI coordinates and represents standards in the United States, while ISO is a network of 157 national standards bodies each representing an individual country. ANSI is the U.S. member body of ISO. X9 is the U.S. representative for the financial services industry through ANSI and has organized the association to adhere to ANSI essential requirements for standards developments and rules of governance. For ISO, X9 is the secretariat of TC 68 and is the lead member body for global financial industry standards. Presently the X9 membership has a wide variety of financial industry standards underway including such topics as entity or party identifiers (LEI), image exchange and quality, cash management BTRS (Balance and Transaction Reporting Specifications), remittance data standardization, mobile banking/payment standard and many data security standards projects.

Upon committee approval, followed by review under ANSI or ISO rules, a proposed standard receives official status by these governing bodies becoming either a published American National Standard or a published ISO standard. Global financial services partners, financial regulators and others cite ISO and X9 American National Standards in rules and in regulation because of their global reach, transparent development and consensus-based process. Following are the scope and some details on a few of the current standards development projects underway:

ISO Standard 20022

Both X9 and its partner organization, ISO TC 68, have worked to build content for this global standard and have seen rapid expansion of the ISO 20022 standards repository. ISO 20022 is the standard that defines the platform for the development of all financial messages. Its business modeling approach allows users and developers to represent financial business processes and underlying transactions in a formal but syntax-independent notation. These business transaction models are the "real" business standards. They can be converted into physical messages in the desired syntax. Actively participating in the work are representatives of more than 34 nations along with multiple global liaison organizations. The 20022 repository

contains more than 300 messages in four categories—payments, foreign exchange, securities, and card/retail and trade services.

Mobile Banking Payments
Applications for Internet-enabled smart phones in the banking services arena are growing in popularity. Many organizations have instituted several apps in transferring money and physical goods purchases with mobile devices. Experts predict the widest applications will take place in developing countries. Here, micropayments via mobile phones should rapidly expand. The multifunctional mobile phone will soon become a "wallet" for many users. Mobile payment systems are the most important activity in need of standardization. ISO now has a subcommittee taking on the role of standards developer for the needed technical elements that will complete its work. Once these standards are complete, rapid adoption of the technical standards is expected.

These beliefs are based on a study by Juniper Research that predicts the international mobile payment market will reach $600 billion in 2013. The consumer benefits of mobile banking are clear, and the financial services industry has an interest to see that customers may easily use the services they have grown accustomed to accessing.

Standards are needed to address geographic hurdles, as well as the different interests of carriers and handset manufacturers. The recently adopted work item call for activity in three main areas:

- Provisioning of bank applications and their management,
- Security, and
- Person-to-person and person-to-merchant sales.

This standardization will address the areas that cannot be handled by individual banks, and applications that are unique to particular institutions will not be included in the standard. The X9/U.S. is leading this work with active expert U.S. participation.

Image Exchange and Quality
X9's Payments subcommittee has developed and improved standards that greatly reduce the amount of handling and consumer reporting in all check transactions. A national standards effort continues to remedy check processing issues among financial institutions in North America. Central to today's check processing is the role *image quality* plays in reducing paper handling and documentation. Now, standards developers are looking to enhance digital recognition that will cover check processing and other payment-related areas of interest. Future support will examine modern methods for measuring dynamic Print Contrast Signal (PCS)[1] and/or Dynamic Contrast (DC)[2] image (ASC TR100-2009 - Organization of Standards for Paper-based and Image-based Check Payments, X9.100-110/X9.7).

X9 Sensitive Card Data Protection
The theft of sensitive card data during a retail payment transaction is increasingly becoming a major source of financial fraud. While thefts of data at all segments of the transaction processing system have been reported, the most vulnerable segments are between the point of transaction device capturing the magnetic stripe data and the processing systems at the acquirer. Therefore, X9 approved a new work item for a standard (to be named X9.119) – Requirements for Protection of

[1]PCS is the ratio of the reflectance of a point to the reflectance of a reference or background region.
[2] A Dynamic Contrast Image (DC Image) is a black/white (binary) image that is derived from a gray level image using a computation method (algorithm) based on PCS measurements.

Sensitive Payment Card Data, Part 1: Using Encryption Methods – and formed a new working group (X9F6-1) to develop a national standard that would standardize the security requirements and implementation for a method to protect this sensitive card data.

X9 Secure Internet Authentication
To support consumer demand and the industry's move towards debit transactions on the Internet, X9 approved a new work item for a standard (to be named X9.122) – Secure Consumer Authentication for Internet Payments. Due to the technical nature of this work, a dedicated working group (X9F6-2) was formed to develop and produce this national standard. The working group has begun the creation of the standard that will provide secure consumer authentication for debit transactions enacted or made on the Internet.

Format Preserving Encryption of Financial Information
Encryption has historically been an expensive technique to deploy in real world systems because of the need to alter the operation of existing systems and applications. Format Preserving Encryption (FPE) techniques encrypt structured data, like payment card Primary Account Numbers or Social Security Numbers, so that the enciphered data has the same format as the plaintext data. This allows encrypted data to be stored and transmitted by the same programs and databases that handled plaintext data without modification. This is the basis of a newly approved standards development project by X9. The working group has begun work on (what will be named X9.124) Format Preserving Encryption of Financial Information. This national standard will fulfill the need for card data encryption techniques that work with existing business processes and systems. It will provide a set of recommendations for use of these techniques within financial systems, and will define a baseline set of security parameters that other standards organizations can use.

Legal Entity Identifier (LEI)
Under the Dodd-Frank Act, the U.S. Treasury organized the Office of Financial Research (OFR) and provides it with the authority to collect data to support the Financial Stability Oversight Council and to set standards for reporting such data. To support the Council in identifying connections among market participants and monitoring systemic risk, the Office intends to standardize how parties to financial contracts are identified in the data it collects on behalf of the Council.

Since government identification of this need, X9/TC68 organized a study group and began preparing a standard fit for purpose and to meet specification and characteristics for a global Legal Entity Identifier (LEI). Currently, an international draft (ISO) standard is balloting for approval at the country member level voting. The resulting standard will be a Legal Entity Identifier (LEI) that will standardize the types and formats of data that is reported. In addition, the standard will include accurate identification of legal entities engaged in financial transactions and facilitate management of systemic risk. A decision on a Registration Authority for the standard is a part of the ISO management process. The benefits and pro-competitive effects of voluntary standards use and application are significant. Voluntary, consensus-based standards have allowed for the systemic elimination of inefficient product differences, provided for interoperability, improved quality, reduced risks and costs and often simplified product development. Standards which are used to develop new products and services promote quality, environmental friendliness, safety, reliability, efficiency and interchangeability. The international study group on Identifiers will continue work on various other identifiers including: review of its current identifiers and their suitability for changing global needs, identification of securities, classification of financial instruments and more to improve and facilitate management of systemic risk.

Lattice-Based Polynomial Public Key Establishment Algorithm
Encryption technology can provide both confidentiality and privacy. Public-key (a.k.a., asymmetric) cryptography is characteristically too CPU intensive for use by computationally limited devices or for high volume transactions, and therefore is typically relegated to managing symmetric keys. On the other hand, while symmetric key cryptography is relatively faster and therefore better suited for computation intensive environments, the complexity of generating, distributing, using and terminating large numbers of symmetric keys can negatively impact operational efficiencies.

The American National Standard X9.98 specifies the cryptographic functions for establishing symmetric keys using a lattice-based polynomial public key encryption algorithm and the associated parameters for key generation. The mechanism supported is key transport, where one party selects keying material and conveys it to the other party with cryptographic protection. The keying material may consist of one or more individual keys used to provide other cryptographic services outside the scope of this standard, e.g. data confidentiality, data integrity, or symmetric-key-based key establishment. The standard also specifies key pair generators and corresponding key pair validation methods supporting the key transport schemes.

The financial services industry benefits from a fast public-key encryption algorithm that offers high security, yet has low processing requirements. The corresponding low memory and low power requirements would enable "appliance cryptography" to protect sensitive data in financial transactions used with portable online and wireless devices for electronic commerce. Furthermore, the proposed algorithm is based on a different, well-studied hard problem from existing algorithms. The availability of the proposed algorithm may protect institutions from breakthroughs in quantum computing or other methods of attack against existing algorithms.

Wireless Management and Security — New Part 3: Mobile Commerce
An X9 working group has begun development of a Part 3 of the Wireless Management and Security Standard dealing specifically with mobile commerce. The mobile environment represents a challenging relationship between the financial services, mobile manufacturers and mobile carrier industries. In addition the added security risk factors consisting of unattended terminals, card-not-present transactions, untrustworthy platforms and persistent wireless connections leaves an uneasy level of assurance for financial institutions, merchants, payment providers and consumers. Part 3 will cover areas such as mobile transactions including sending and receiving messages for payments and banking, mobile payments for person to person (P2P), person to business (P2B) and small business to business (SB2B) including credit card, debit card and electronic funds transfer (EFT) transactions.

Remittance Data
Remittance information is defined as data that is provided by a customer to a seller that explains the purpose of the payment. The seller then uses this information to reconcile the payment.

Currently within the industry there is a complex surplus of standards and approaches for providing this automated remittance information. As a result, X9 and the Federal Reserve Bank of Minneapolis sponsored a Remittance Workshop in June to bring together remittance specification developers, corporate customers and other parties interested in improving the automated reconciliation between payments and remittance data. The specific purpose of this "by invitation only" workshop was to recognize the complex surplus of remittance standards, inform standards developers and other interested parties about the diversity of remittance standards, review existing remittance standard formats to identify differences and similarities, identify key corporate user "pain

points," talk about the pros and cons of moving towards a single format in the U.S. for remittance processing and develop a roadmap and next steps for moving forward to address these issues.

As open, transparent and consensus-based standards become more necessary to the functions of the financial services industry, more not less standardization will be relied upon for future challenges and opportunities. In X9, members gain the advantage of understanding new ideas, technologies and implementation guidance long before the competition may decide or be mandated to follow the concepts behind X9 standards. This lead-and-not-follow mindset offers the ability to anticipate and accommodate new standards development.

Cynthia L. Fuller

Executive Director of the Accredited Standards Committee X9, Inc., Ms. Fuller currently manages two secretariats for national and international bodies that develop and manage standards for the banking and financial services industry. Prior to her work with ASC X9, Ms. Fuller was a leader in the Fee Management Division at the Johns Hopkins University School of Medicine in Baltimore, Maryland. And, prior to Johns Hopkins, Ms. Fuller served as a management consultant to medical and dental professionals on practice management. Ms. Fuller holds degrees from The Ohio State University, a Bachelor of Business Administration and a Masters of Science.

Regulation in the Financial Services – It doesn't require the government to make it work.

By Bob Russo, General Manager, PCI Security Standards Council

When we talk about regulation in financial services, we often categorize it in two forms, government mandated regulation, like SOX or GLBA, and voluntary or industry regulation, or self-driven standards, such as international standards like ISO 27001, and the Payment Card Information (PCI) Security Standards.

While all of these have benefits, I want to stress that industry self regulation WORKS. I know that in the past there have been rumblings and suggestions that industry regulations like PCI are ineffective or motivated by the agenda of certain industries. I'm proud to say, however, that five years after the PCI Security Standards Council was formed - and the first consolidated update to the PCI Data Security Standard (DSS) was issued - that self-policing can and does work. And we've got some great proof points to illustrate why it's working. The industry continues to use the real-world feedback from professionals across the payments chain to make the most prescriptive set of data security standards available today and which form the basis of the best practices that are fundamentally proven to reduce payment card fraud globally.

Indeed, both the Trustwave, Verizon Business and the UK Payments Association annual reports show payment card fraud receding and even falling to historic lows. Recent figures from the UK Cards Association showed that banking industry initiatives, including PCI, have been successful in decreasing the volume of card and bank account fraud. Of particular interest to us at the PCI Security Standards Council was the finding that payment card fraud losses in 2010 reached their lowest levels since 2000, and have made significant improvement from their all-time high just three years ago in 2008. Overall, these numbers suggested that total fraud losses on UK cards fell by 17 percent alone over the preceding year.

The Ponemon Institute's 2011 PCI DSS Compliance Trends Study found that PCI compliant organizations suffer fewer data breaches. Organizations reporting compliance with the standards has increased tremendously over the last year and the volume of breaches reported in the Verizon Data Breach Investigations Report (DBIR) decreased close to a hundredfold from their 2008 peaks.

These are fantastic positives and proof points that organizations are beginning to understand the very real equation: that the cost of compliance is significantly less than the cost of a data breach incident. Just look at all the possible issues you may have to deal with after a breach:

- It's estimated that each compromised record will cost a company between $90 and $300. This does not include the costs of lawsuits resulting from the breach or other ancillary costs such as remediation efforts. There may be other legal ramifications as well, such as governmental intervention. As an example, it's estimated that the total cost of the TJX breach will be in excess of $250 million.
- Ponemon Institute suggests that data breaches cost U.S. companies about $214 per compromised record in 2010, and averaged $7.2 million per breach event. You, your company, your shareholders or investors, every part of your organization ends up having to pay when you let one of these bad guys in. You quite simply are handing over the keys to your bank account.

The successful decrease in fraud in each of these reports also illustrate that organizations are understanding that breaches cost money and that your best defense against data breaches are the PCI Security Standards.

As such, we see a tremendous and renewed focus on training and education within organizations to further decrease these rates of fraud, and close the security gaps that have led to many breaches historically. While many organizations in the past have tried to combat fraud and protect sensitive information through technology or processes, there is a third pillar - people - that must be included in order to be truly successful at securing card data. This is an area where the PCI Security Standards Council can help.

The PCI Security Standards are designed to protect payment card data within merchant and service provider environments and require appropriate measures to protect any systems that store, process and/or transmit cardholder data. The PCI Security Standards Council manages these standards and provides educational resources to arm organizations with the knowledge, skills and tools to help you secure your data.

Education plays such an important role in helping us help you secure your data that we added a new PCI Awareness training to our offerings, a high-level basic introduction to PCI open to anyone who wants to learn and understand what PCI DSS is, its impact on an organization and the importance of PCI compliance. This class is also available online and designed for ultimate flexibility so you can take it wherever, whenever.

PCI is not a finance issue, or an IT issue, or a risk issue, it is cross functional, and it fundamentally relies on people driving it. And our hope is that with Awareness training, organizations can ensure that they build a base level of understanding on how to best protect cardholder data across different business areas. This is truly the core of the people aspect of security.

Another unintentional benefit of the standard that we are seeing across the board, but particularly in the financial services space is that PCI compliance projects can drive or fund other network and information security projects. In fact, in a recent survey of IT decision makers conducted by our Board of Advisors member Cisco, 87 percent of IT decision makers indicated that they believe PCI compliance is necessary in today's business world. Sixty percent of respondents also indicated that the PCI requirements can help them leverage PCI compliance programs by driving budget for other IT or security-related projects. Financial services firms have been consistently ahead of the curve on this one, with more than 72 percent of respondents leveraging their PCI programs to shore up their overall security efforts – the highest of any vertical. This is important, as the threat landscape has shifted. In the Verizon 2011 Data Breach Investigations Report, we see an important trend in data theft. That is the growing number of organized crime attacks attempting to steal data. External breaches are largely the work of organized criminals and these external breaches resulted in 99+ percent of all records exposed in their study. These guys are the ones going for the largest volume of data.

Internal breaches have shifted a bit too. We all used to think that internal breaches were usually caused by someone losing a laptop, or USB drive somewhere, but that is not the case, with 93% of internal breaches being deliberate attempts to steal data. So we can all see the trend here. We know that organized, persistent criminals are out there looking to commit attacks specifically designed to steal valuable payment card data to turn into cash for their operations.

So how do we, as an industry respond to this shift in threats? Through the evolution of the PCI Standards and your feedback on supplemental guidance that helps to thwart, alert or minimize the likelihood of data breaches occurring in your organization. We update and create the newest versions of the standards based on the real-world experience from hundreds and thousands of folks like you, living security every day. To enhance payment account data security by driving education and awareness of the PCI Security Standards, we rely on hundreds of organizations around the world.

The foundation for providing this feedback is our Participating Organizations, companies representing all sectors of the industry - from merchants and service providers to payment device manufacturers and software developers, financial institutions and processors - who are committed to influencing credit card security through involvement in the Council. Built into the standards lifecycle is a feedback loop, where we proactively solicit organizations on ways to better evolve the current standards. One example from the last feedback period was a request for additional clarification on where elements of cardholder data must be protected when stored in conjunction with the Payment Account Number (PAN). Our technical working group reviewed this, presented a proposed change back to the Participating Organizations and the official language in the newest version of the PCI DSS 2.0 now includes an updated table with additional clarifications so that all can better understand the nature of that requirement.

We also get feedback and guidance from Special Interests Groups (SIGs), groups made up of our Participating Organizations and formed by the Council to assess specific, payment technologies within the scope of the PCI Data Security Standard (PCI DSS) and the security of credit card data. Working with the Council these groups have delivered additional, supplemental guidance on technologies such as point-to-point encryption, EMV, wireless and best practices to avoid card skimming fraud. The system works because of this feedback, and because of your involvement. But there is much more to be done.

While last year we saw a drop in fraud losses, where will we end up in 2011? We are only half way through the year, and already have seen the impact of a series of global, massive data breaches. What these events prove is that merchants, processors and others involved in the payment chain must take direct action to place security soundly into their day-to-day business efforts.

This year presents a tremendous opportunity for you in the financial services industry to be involved in the shaping of the next iteration of the standards and where we go globally from here. This year, those of you already involved in the PCI community have voted in a new Board of Advisors for the PCI Council. The 2011-2013 PCI Board of Advisors will provide strategic and technical guidance to the PCI Security Standards Council that reflects the varied and unique industry perspectives of those across the payment chain. In addition to advising on standards development, the Board of Advisors plays a critical role in soliciting feedback and ideas, leading Special Interest Groups (SIGs); and helping the Council fulfill its mission to raise awareness and adoption of PCI Standards. Representatives from the financial service industry include Barclaycard, Cartes Bancaires, Citi, European Payments Council, First Data Corporation, Heartland Payment Systems, JPMorgan Chase & Co. and TSYS.

Next, we've got the forthcoming PCI Community Meetings. These important events offer Participating Organizations and Council stakeholders the unique opportunity to participate in interactive sessions to discuss and provide feedback on their implementation of the newest versions of the PCI Security Standards. The Council will provide brief updates on current initiatives, including the latest guidance documents on payments technologies, with the majority of this year's

sessions structured as question and answer forums and industry networking sessions. This is in addition to the popular welcome receptions where attendees are able to meet and network with payment card security industry leaders and stakeholders from around the globe. These meetings will be held in Scottsdale, Arizona on September 20-22, 2011 and London, United Kingdom on October 17-19, 2011. These meetings are vital as we begin to look at all future assessments being completed against DSS 2.0 by January 1, 2012. Right after the Community Meetings begins the important feedback period, where we hope to get your vision and input on the next iterations of the standards and the additional guidance you would like to see.

Your feedback and participation is why self regulation works. Keep it coming in the next year and together we will succeed in reducing payment card fraud globally.

Shared Assessments Background

By Michele Edson, Shared Assessments

Traditionally, ensuring the quality of service provider controls has been cumbersome and expensive for both the service provider and the client. Teams of specialists were hired to personally inspect a service provider's controls, traveling for several days at a time, often to far-flung destinations. On the service provider's side, personnel had to be devoted for weeks at a time to client inspections and detailed information requests. With potentially hundreds of providers serving hundreds of clients, the redundancy of effort is often enormous, carrying with it significant unnecessary expense.

A decade ago, senior financial services leaders agreed that they needed to standardize risk management for IT outsourcing. Through the BITS IT Service Providers Working Group, these executives created a seminal document, the *BITS Framework for Managing IT Service Provider Relationships*. The *Framework* standardized risk management practices for financial services IT outsourcing, including identifying appropriate vendors, conducting due diligence, contractual considerations, ongoing relationship management, disaster recovery and cross-border considerations. In 2003, the IT Service Providers Working Group released a companion to the *Framework,* the *BITS IT Service Providers Expectations Matrix*. The *Matrix* outlined service provider practices, processes and controls relevant to the financial services industry and regulatory requirements.

In 2005, a small group of leading financial institutions, in collaboration with leading service providers and the Big Four accounting firms, conducted a pilot program to see how a group of clients and service providers could achieve efficiencies if the clients agreed to share the kinds of information sought in the *Matrix*. If the companies – led by Bank of America Corporation, The Bank of New York Mellon, Citi, JPMorgan Chase & Company, U.S. Bancorp, and Wells Fargo & Company -- could agree on a defined set of questions whose answers could be shared, clients and service providers would achieve significant efficiencies and cost savings.

The Shared Assessments Program was launched in 2006. BITS engaged strategic consulting company The Santa Fe Group (www.santa-fe-group.com) to manage the Program, and it opened its doors with a meeting of 100 participants from financial institutions, service providers, regulatory agencies, assessment firms and others in New York City at the headquarters of PricewaterhouseCoopers. The *Wall Street Journal* called the Shared Assessments Program "a strength-in-numbers approach to guarding customers against security breaches."

In many cases, these new outsourced services are functions that hold sensitive customer information. Financial institutions that engage in these relationships are legally responsible for monitoring the service provider's controls for privacy, security and business continuity. In other words, while a financial institution can outsource the service, it can never outsource the risk associated with that service.

The Shared Assessments Program (www.sharedassessments.org) is a member-driven consortium of corporations in a range of industries, IT service providers, and assessment firms, including the Big Four accounting firms. With more than 55 participating companies, the Shared Assessments tools are in use in 115 countries. Three thousand individuals around the globe download the tools annually.

Shared Assessments' dual mission is to:

1. Offer rigorous standards for managing risks associated with security, privacy and business continuity controls in IT outsourcing relationships.
2. Provide its members with critical knowledge about trends in global outsourcing.

By 2008, the Shared Assessments Steering Committee was seeing corporations in other industries use the Shared Assessments tools. Healthcare companies were facing new requirements related to patient data, and other industries, like retailing and telecommunications, were finding themselves increasingly intersecting with customer data for which they had to be responsible. In fall of 2009, Shared Assessments officially expanded its membership to include industries outside of financial services. Today users of the Shared Assessments tools include financial institutions as well as universities, government entities, healthcare organizations, manufacturers, pharmaceutical companies, retailers, telecommunications companies, and others.

The financial crisis and recession have changed the way companies around the globe do business. Corporations are finding new ways to manage and predict risk. Senior managers are changing the way they oversee departments and enterprises. To save costs and build efficiencies, some companies are restructuring, in part through outsourcing.

A Global Community

Today's Shared Assessments Program is a source of technical standards for thousands of organizations, a resource for insights about domestic and international trends in outsourcing, and a global networking hub for hundreds of risk management and outsourcing professionals. Members meet monthly through the Shared Assessments Member Forum teleconferences and access each other via a LinkedIn discussion group. Members also have access to each other through in-person meetings and by contacting each other directly for advice and perspectives on a range of outsourcing issues.

Each year, Shared Assessments and The Santa Fe Group host the Shared Assessments Summit. A consistently sold-out event, the Summit brings together members and nonmembers for a discussion that balances "big picture" global outsourcing trends with tactical advice about using the Shared Assessments tools. In March 2011, keynote speaker Atul Vashistha, CEO of NeoGroup, talked about outsourcing's evolution from labor arbitrage to a vehicle for operational transformation. Richard Levick, president and CEO of Levick Strategic Communications, discussed the fallout from major PR disasters involving outsourced services. Shared Assessments Steering Committee Member Niall Browne, CISO of LiveOps, discussed risk management in cloud environments. Other sessions focused on social responsibility in outsourcing, technical issues, and member case studies. A sold-out pre-conference workshop introduced members and nonmembers to the basics of incorporating Shared Assessments' standards into vendor risk management programs.

The Shared Assessments Program continues to offer two industry-standard tools for managing vendor risk: the Standardized Information Gathering Questionnaire (SIG) and, for onsite assessments, the Agreed Upon Procedures (AUP). These tools are maintained by the Technical Development Committee of the Shared Assessments Program, a group of privacy, information security and business continuity experts dedicated to promoting global adoption of the Shared Assessments standards. Shared Assessments is governed by a Steering Committee chaired by Charlie R. Miller of the Bank of Tokyo-Mitsubishi UFJ, Ltd. Still clear in its original mission to reduce assessment costs, the Shared Assessments tools inject speed, efficiency and cost savings into the service provider control assessment process.

In addition to its members, the Shared Assessments Program has strategic alliances with global associations including the National Association of Software and Services Companies (NASSCOM) and the Securities Industry and Financial Markets Association (SIFMA). Shared Assessments also continues its affiliation with BITS. The Santa Fe Group manages the Program, providing a trusted forum for dialogue and collaboration among all stakeholders on issues that matter to outsourcers, their service providers, assessment firms, regulators and others; The Santa Fe Group's chairman and CEO is Catherine A. Allen, the former founding CEO of BITS. Together, Shared Assessments' diverse membership and stakeholders work to increase awareness and adoption of the Shared Assessments tools across industry sectors and around the globe.

Activities
As part of its mission to provide its members with knowledge and insights in global outsourcing trends, Shared Assessments offers opportunities for members to address global risk management challenges through its working groups and committees.

Cloud Working Group
The Shared Assessments Program began addressing cloud computing in 2009 when members added six new procedures to its on-site assessment tool (the AUP) and inserted cloud-relevant questions into several sections of the Shared Assessments questionnaire (the SIG). In 2010, the Shared Assessments Cloud Computing Working Group published Evaluating Cloud Risk for the Enterprise: A Shared Assessments Guide.

Led by Niall Browne, CISO of LiveOps, the Cloud Computing Working Group meets regularly to discuss developments in cloud technology that affect risk management. This group works with the Shared Assessments Technical Development Committee to make updates that reflect the growing importance of cloud computing across the IT landscape. The Working Group also collaborates with the Cloud Security Alliance, a not-for-profit organization whose mission is to promote best practices for security in cloud environments.

PHI Project
The PHI Project is a cross-industry group of members and nonmembers that is exploring how to protect patient health information and better understand the financial harm caused when protected health information (PHI) data is breached, lost or stolen. Led by the American National Standards Institute (ANSI), via its Identity Theft Prevention and Identity Management Standards Panel (IDSP), in partnership with the Shared Assessments Program and the Internet Security Alliance (ISA), this project was created to promote greater clarity on these issues so that the healthcare industry can:

- Make better investment decisions to protect PHI
- Improve its responsiveness when patient information is compromised

ANSI/Shared Assessments/ISA PHI Project members are a cross-industry group of more than 100 experts from data security companies, identity theft protection providers and research organizations, legal experts on privacy and security, standards developers, and others. Together, these individuals are working to develop a formula that healthcare organizations can use to determine the economic impact of any disclosure or breach of PHI. The group's findings will be published in a report targeted at those responsible for and entrusted with protecting and handling PHI.

Rick Kam, president and co-founder of Shared Assessments member company ID Experts, chairs the PHI Project.

Technical Development Committee

The Technical Development Committee (TDC) is made up of chief information security officers, chief privacy officers, and subject matter experts who are motivated to help build and sustain Shared Assessments' rigorous standards. TDC participants include experts from Industry, Service Provider, and Assessment firm members, including the Big 4 accounting firms (Deloitte & Touche, Ernst & Young, KPMG, and PricewaterhouseCoopers), which serve as Technical Advisers to the Shared Assessments Program.

The Technical Development Committee is led by The Santa Fe Group Senior Consultant Brad Keller brad@santa-fe-group.com.

For more information about Shared Assessments, visit www.sharedassessments.org or contact Michele Edson, michele@santa-fe-group.com. To learn more about The Santa Fe Group, visit www.santa-fe-group.com

Redefining Static Analysis, A Standards Approach

By Rama S. Moorthy, CEO,and Ioan (Mike) Oara, CTO, Hatha Systems

Introduction: What is Static Analysis?
There are two ways to gather information about a system and analyze it for security or other purposes: one is to look at it as it operates and the other is to look at its artifacts. These two methods correspond to dynamic and static analysis. Although the dynamic approach has often been the easier path to take for analysis, it is the static approach that can render more comprehensive results.

Take for example the case in which a security analyst tries to determine if there is a particular user interface in which certain confidential information (such as a customer personal address) is displayed. With dynamic analysis, one would have to execute all possible operations of the system, enter any possible combination of codes, and even try to supply values that do not make sense. This task may be overwhelming and may never provide a 100% assurance that the confidential information would never surface. However, through static analysis, which involves looking either at the source code or at information extracted from it, the analyst can discover with absolute certainty if the customer personal address is displayed somewhere. Moreover, if it is displayed, the analyst may also find the precise combination of input data and user actions in which this is happening.

While static analysis could be as simple as looking at the source code of an application, the last decade saw the emergence of specialized tools which deliver both high productivity and precision. The amount and complexity of data make such tools indispensable. To perform static analysis, such tools usually go through two phases:

(a) Data gathering through the parsing of the source artifacts
(b) Specialized analysis that digests the information and presents it in a useful form.

The specialized analysis could render diagrams which help the analyst get a view of the application at any level of detail. The following are examples of those views:

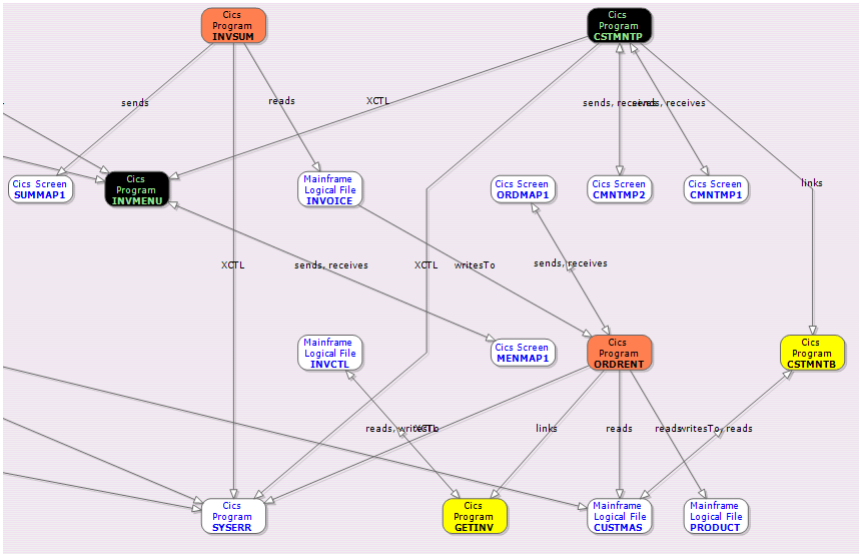


Figure 1: System Architecture

A system architecture diagram indicates how various platform components interact. In the Figure 1 diagram, one can see how particular programs interact with the screens and read or write data to files.

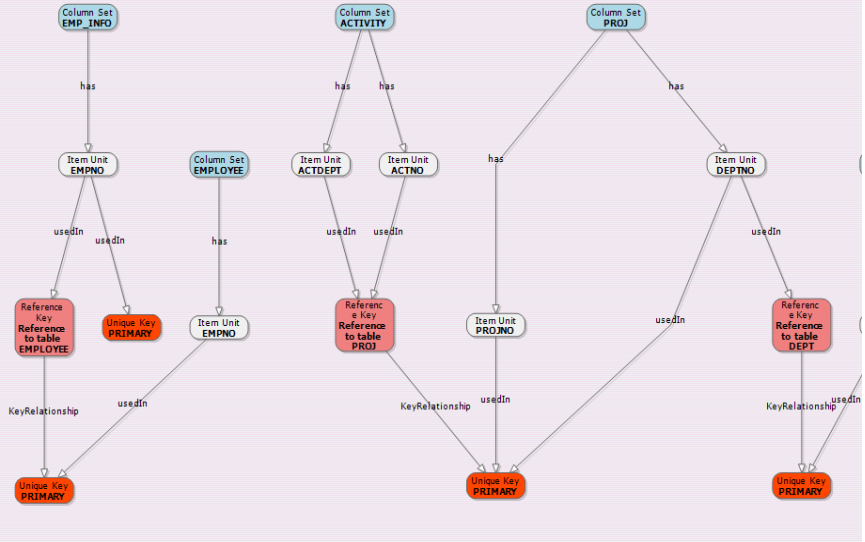


Figure 2: Data Architecture

Some Static Analysis tools are capable of automatically extracting database schemas and discovering complex data relationships. Figure 2 above is an example of that extraction.

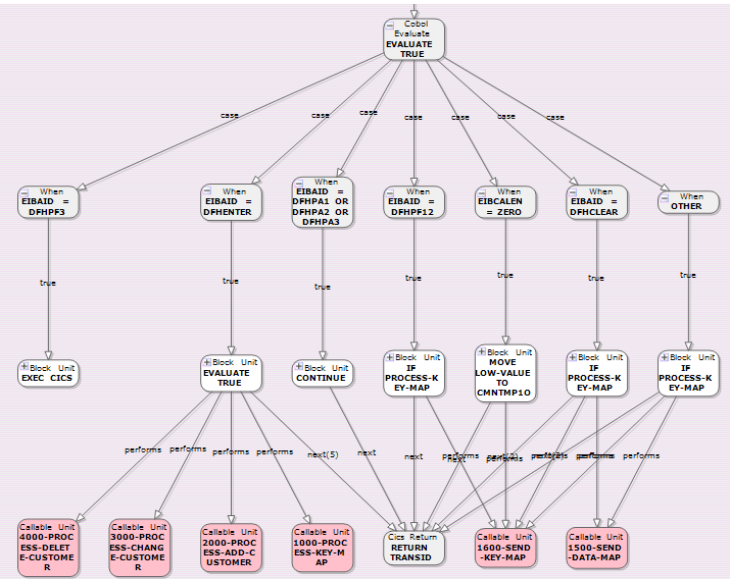


Figure 3: Control Flow diagram

A Control Flow diagram, as in Figure 3 above, helps discover the various paths through the code and the conditions on which they branch. This in turn helps discover business rules, data validations or process composition.

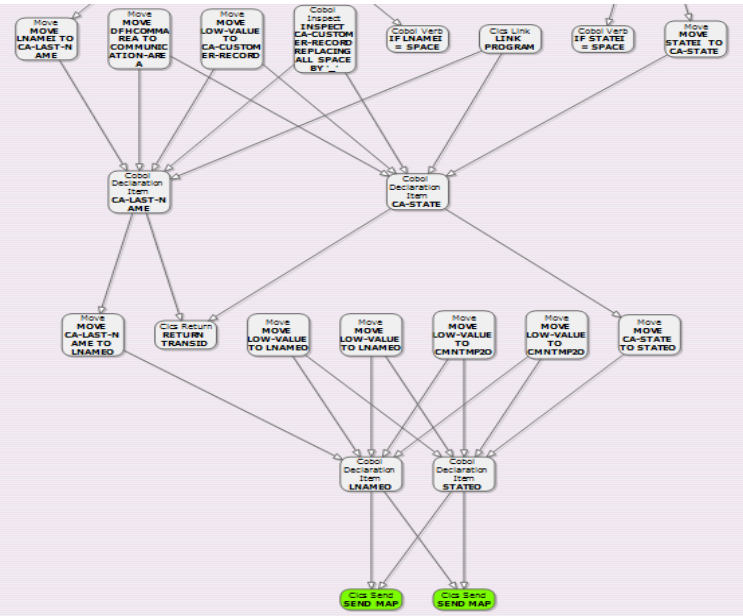


Figure 4: Data Flow diagram

A Data Flow diagram, as in Figure 4 above, helps discover the paths of data through the application. In particular, one may discover what data is presented to the operator and what the data origin is.

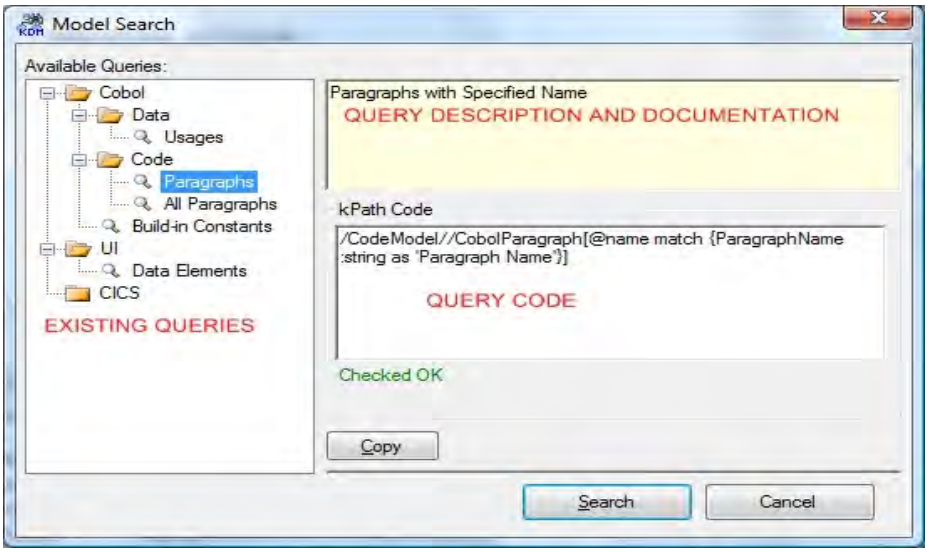


Figure 5: Static Analysis queries

A Static Analysis tool may also provide the analyst with query capabilities. Figure 5 is an example of how such queries are defined. Various tasks, such as business rules extraction or code weakness discovery can be aided with the use of a static analysis tool.

Engineering Applications into Securely Composed Systems

One particular strength of static analysis tools is the capability to analyze the strengths and weaknesses of a composed system. Modern paradigms require that applications work in concert as opposed to separate stacks. As many applications were developed in the past without a requirement

for connectivity, bringing them together requires extensive analysis, which is helped by static analysis tools. They can help with a number of distinctive tasks.

1. Discover if the data provided by one application is consistent with the data required by another. This involves data formats, data validation rules and semantics of data.
2. Discover if the security rules of one application are consistent with the security rules of another. For instance, one may require a special authentication, which is not required by another.
3. Discover if different components are at similar levels of assurance, such that one will not degrade the other.

One simple example refers to the input validation rules. One component application may accept a customer regardless of age, while a second may impose some age restrictions. If the first one lets a customer pass and makes a request to the second, this in turn may end up processing unqualified customers. A static analysis tool may be able to collect all validations from both applications and compare them for consistency.

Issues with Static Analysis Tools

There are a number of issues that continue to impact the advancement of comprehensive tool aided analysis. The speed of innovation in the development of new languages and technologies, although providing tremendous efficiency and ease to the development community, has forced the discipline of tool aided static analysis to focus on only a narrow set of issues (e.g., extraction of code weaknesses, business rules extraction). Such solutions address only isolated issues for a few established languages, and fail to offer a comprehensive approach capable of simultaneously viewing code, architecture, platform, data, business/operational rules and business/operational processes. All of these characteristics of a system play a part in fully understanding the state of a given system. In other words, full contextual knowledge of any system being analyzed is critical to providing a comprehensive view of its strengths and weaknesses. Additionally, the state of constant change in software also dictates the need for this knowledge to be extracted on-demand. Given the heterogeneity of languages and the continuous state of change in technology, the optimal way to address the knowledge extraction and automated static analysis is to use standard models. Standard models allow for the use of a common language (ontology) and can be applied to build out an eco-system of automated tools, regardless of the system being analyzed or the type of analysis being performed. Once a standard representation is used, tools which are otherwise specialized in either particular technologies or in particular types of analysis can come together and complement each other. Even for specialized tasks, such as the discovery of code weaknesses, it was determined that different tools deliver slightly different results. Using them in combination would assure a more comprehensive and higher quality analysis of a particular system.

One particular area in which the standards may prove decisive is related to the issue of composable systems discussed previously. If one tries to integrate two systems built on separate technologies, it is highly probable that while analysis tools may be available for both technologies separately, no tool has to date been capable of dealing with both of them. However, if the two useful tools are built on the same standard model, their data, results and conclusions may be integrated.

Standards Progress

Over the last seven to eight years, a group of industry leaders have been addressing the need for international standards that knit together to provide a comprehensive analysis framework. This effort has been driven by the modernization community which requires full system knowledge of the 'as is' system, a critical component for both analysis and reuse when migrating the system. This

community is entrenched in system engineering methodologies and process, and has brought that same rigor to addressing software analysis as an engineering effort. The result is a number of standards that set the stage for comprehensive static analysis. The standards include:

Knowledge Discovery Metamodel (KDM): an ISO/OMG standard providing ontology (a set of definitions) for system knowledge extraction and analysis. KDM provides a framework for the capture of code, platform and other software system characteristics. This further allows the extraction of data flows, control flows, architectures, business/operational rules, business/operational terms, and the derivation of business/operational process; the extraction can be delivered from source, binary, or byte code. Additionally the intermediate representation of the extraction is in executable models creating the possibility of simulation and code generation.

Business Process Modeling Notation (BPMN): an OMG standard delivering a modeling notation used to capture business/operational processes in support of system and organizational process simulation and analysis. It is used today to capture both human and IT system processes for the purposes of simulating environments both 'as is' and 'to be' for software modernization. This notation is compatible with KDM so that system extraction can be represented in BPMN for gap analysis of the current state of the system vs. what is thought to be the current state of the system – critical for modernization and compliance.

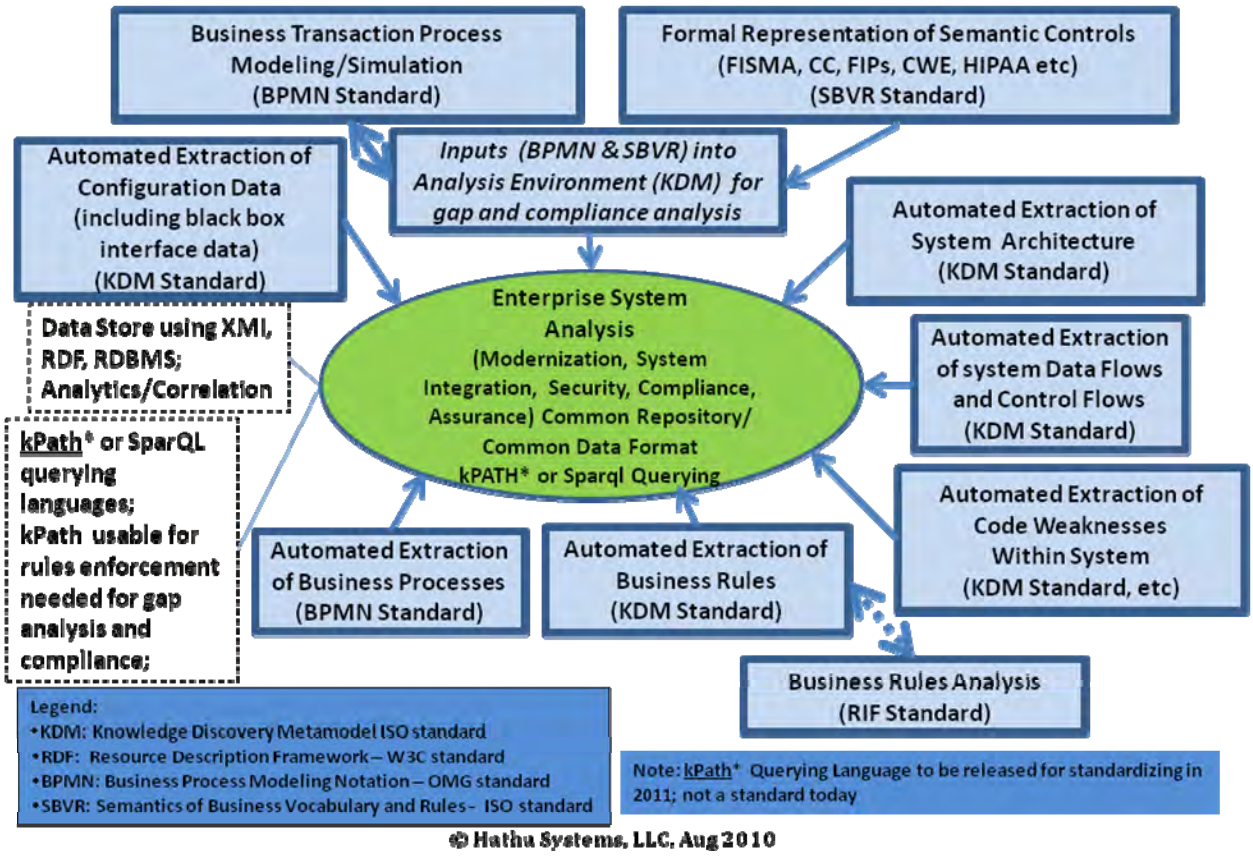
Rules Interchange Format (RIF): W3C standard, this standard delivers representation used for specifying, analyzing and exchanging information about business rules. Once captured in this format, business rules may be also be used in simulation, gap analysis and compliance analysis. The analysis of business rules is also an important aspect of application modernization.

SBVR (Semantics of Business Vocabulary and Business Rules): An ISO/OMG standard, this specification provides a structured process for formalizing, in natural language, the existing English language representation of compliance points. The standard enables the various compliance specifications (e.g. FISMA, HIPAA, SOX, FIPs, CWEs, etc) to be formalized reducing the room for interpretation from organization to organization when implementing the compliance and auditing requirements.

Data/Metadata Storage Standards (old and new): With the emergence of the standards noted above and the need for storing this information for analysis, a set of storage standards needed to be embraced. XMI, RDMBS, and RDF (Resource Description Framework) are the three formats that are compatible with these standards. RDF - perhaps the least known of them - is a W3C standard that is compatible with KDM and BPMN. There is a specific approach in the standard called RDF triple store which is currently being used in semantic web applications. The value of RDF is that it can manage large amounts of data and metadata which is critical for doing comprehensive static analysis.

Knitting of the Standards for a Comprehensive Static Analysis Approach

The diagram below provides a pictorial representation of the system information that is extractable using the various standards and how the standards knit together to deliver the foundation for software system knowledge extraction and comprehensive static analysis.



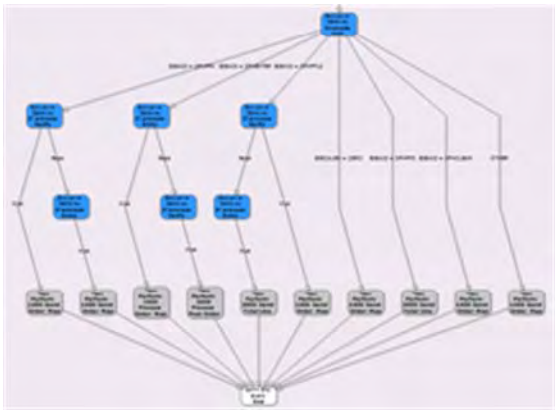
Possibilities when automated static analysis tools embrace these standards:

1) Business/operational logic can be extracted to derive business/operational processes into a BPMN format for documentation, re-architecture (including SOA and Cloud enablement), gap analysis and migration purposes.
2) Rules can be extracted and correlated with business/operational terms and processes for 'as is' system analysis.
3) Rules extracted in RIF format could be used to generate code or may be migrated to a business rule engine.
4) System architectures, data flows and control flows associated with them can be extracted and represented visually. These representations may be used to document the 'as is' system for the purpose of modernization, compliance or security analysis.
5) Code weaknesses can be discovered and then associated with the data and control flows in which they occur in order to determine their possible impact for security, safety, etc. within the context of a specific system. While various technologies aid in the discovery of weaknesses, standards-based static analysis approaches can help place them within a process or architecture context. This in turn can help to better estimate their impact and in turn risk management.
6) Compliance points or controls can be represented in SBVR to formalize each control, then expressed in kPath queries (the KDM querying language – planned for standards release) and placed in a reusable repository for extracting compliance knowledge of the system. This effort can aid in creating a set of institutionalized compliance queries to be used repeatedly in the system lifecycle of a given organization.

7) Configuration data can be extracted in a KDM repository for those components that do not have source code, making them part of the overall system analysis for security or modernization purposes.

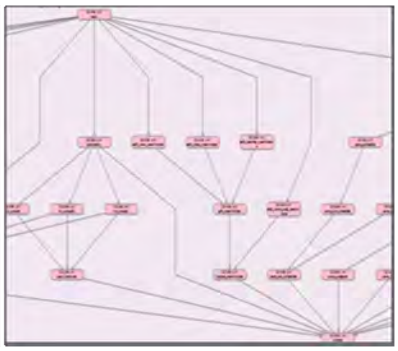
The screen captures below show views from a standards compliance static analysis tools environment:

Business/Operational Process Derivations:



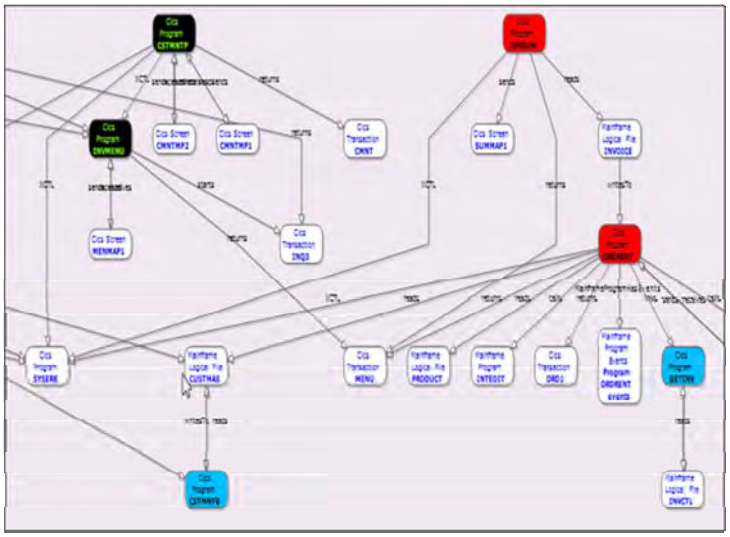
System and Data Architectural Extraction:

Control Flow, Call Map, & Data Flow Extraction

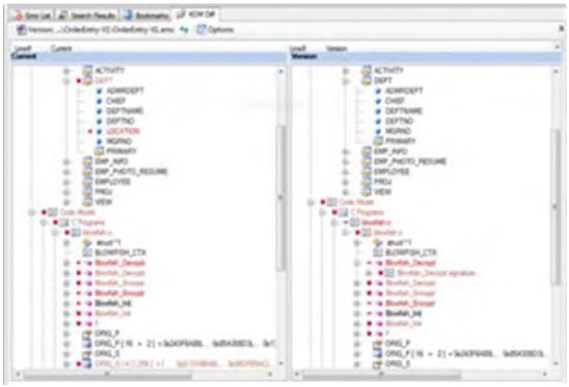


Screen Flow and Screen View Extraction:

Software System Layer Identification: Valuable for function or architectural extraction for security, safety, or SOA enablement or other applications requiring an analysis of functional layers within a system:



Versioning Analysis: The extraction of a baseline system and a new version, valuable for software maintenance impact analysis (e.g. security or safety), compliance.



Conclusion

Both large and small players in the software world have been adopting the various standards discussed above. There is an eco-system forming that brings together a set of tools that can

provide knowledge extraction and analysis which can be integrated using a common data format for better correlation and comprehensive static system analysis.

About the Authors:

Rama S. Moorthy is the Chief Executive Officer and Founder of Hatha Systems, a company providing automated analysis solutions for software systems modernization, compliance and security engineering, built on a foundation of international standards. She has over 22+ years of experience in creating new products, markets, and standards as well as running large revenue generating organizations at Sun, AMD, and Siemens. She has been a content contributor to the Department of Defense Software Assurance and Supply Chain efforts. She is a principal author of the NDIA – Engineering for System Assurance Guide, the DoD Supply Chain Risk Management (SCRM) Key Practices Guide as well as the SCRM NIST-IR. She has a BSEE from Purdue University and an MBA from Vanderbilt University.

Ioan (Mike) Oara, the Chief Technology Officer at Hatha Systems, is one of the veterans of the discipline of Application Analysis and Modernization. Mike started his career in early 80's working in the financial industry in New York. Over the last 20+ years, Mike has been developing technologies and holds several patents in the area of application analysis and modernization. He pioneered new solutions for business rule extraction, creating robust and practical extraction methodologies. At Hatha Systems he continued his innovations through the development of the next-generation of analysis and modernization solutions. Mike has published many articles focused on modernization and static analysis. Mike has a MS in Mathematics from the University of Bucharest.

Improving Information Security & Privacy Assessment Methodology: How to Gain Independence from Competing Standards

By Michael Sukkarieh, Citigroup

Introduction

Today, organizations that conduct Information Security & Privacy (IS&P) Risk assessments are relying on methods that range from guesswork to highly subjective self-assessments to triage processes that must undergo a risk assessment and rely on external standards to build their assessment instrumentation. For large organizations, this can be a taxing overhead and present a challenge to settling on an IS&P standard for adoption and other risk assessment impacts throughout the risk assessment lifecycle. This article will propose a method for assessment as part of the System Development/Deployment Lifecycle Process (SDLC) that works independent of any specific industry standard, leverages existing processes and may reduce inefficiencies and some costs associated with current assessment methodologies.

Known Challenges

From a practical viewpoint, information security & privacy professionals performing risk assessments face some or all of the following challenges when selecting IS&P standards for assessment and evaluation:

Causing "Social Inertia": When large organizations undergo a costly and lengthy evaluation period of an IS&P standard to adopt for the organization, it is expected that the risk assessment process changes and will trickle down throughout the organization. Unfortunately, in many cases, when standards undergo a major change they become a selling point for consulting services that in turn push organizations to adopt too quickly. Changes in standards may in some cases necessitate a risk assessment process update, but not always. A side effect to these changes is "social inertia" which summarizes a degree of resistance to change across the organization creating greater focus on change rather than identification and mitigation of risks.

Loosely Coupled Information Security Assessment Process with a System Deployment/Development Life Cycle (SDLC) Process: The lack of an integrated information security assessment process as part of the SDLC is causing at least an inefficient process and at worst many unnecessary and costly re-assessments at the resource deployment stage. The fact that most organizations have multiple methods to assess, develop or deploy resources that support a process in a multi-dimensional relationship, makes it difficult to leverage existing assessments or other processes (e.g. Application Vulnerability Assessment) that can make the assessment more efficient.

Lack of Common Assessment Methodology Based on Risk Rating: In current information security risk management literature, risk measurement models are discussed as a function of the likelihood of an event happening and the business impact of the outcome of that event. When reviewing current literature, we found there are several standards, such as ISO 13335, COBIT, and COSO, that discuss risk management and briefly touch on risk measurement. These standards suggest using qualitative methods to assess risk and provide little guidance on how to capture risk

results and how to act on those results in a clear and repeatable manner. These standards recommend using qualitative ordinal scales to measure likelihood of threat events and business impact of threat events and using that as a basis to estimate risk. Another example that has become a de facto standard to assess resources is the Common Vulnerability Scoring System (CVSS) methodology. However, its major disadvantage is its focus on technology resources and that it cannot easily assess other types of resources such as human resources or third parties.

Existence of Multiple Standards and Checklists: One of the key issues facing IS&P professionals are the multitudes of "Checklists" based on multiple industry standards that are put together to address an immediate need. These "Checklists" are not, by definition, flexible in either their composition or their administration. Although their purpose is to act as an objective instrument to evaluate the information security and privacy posture of a resource, they are often very subjective with no data useful for quantitative evaluation. In the case where there are clear variables to be evaluated, there is no real effort to prove their statistical independence.

Proposed Methodology

Key Baseline Assumptions

For the purposes of this article, we assume that organizations have the following:

1- An assessment methodology that involves determination of an inherent risk of a resource (e.g. business application, third party, a network infrastructure equipment) with an ordinal rating scale of three (i.e. low, medium and high)
2- A set of control assessment "checklists" based on specific or open-ended information security questions used for information security and privacy assessments.
3- An integrated risk rating per identified control deficiencies with a basic channel of communication to those who need to address them and track them to closure.
4- An up to date inventory of resources.

The purpose of this proposed methodology is to increase the degree of efficiency of the process and decrease the level of dependency on IS&P standards, while improving the quality of assessment and improving cost efficiencies for the organization. The following steps are proposed as part of an overall assessment flow:

Information Security Review (ISR) Event Evaluation Process

This step applies to resources that are not NEW, or that will be NEWLY deployed. The purpose of this step is to determine the depth of the assessment that needs to be completed following an SDLC process.

ISR Instrumentation (ISRI)

The ISRI is a standardized set of detailed questions that cover a range of technical and non-technical control domains. These questions are not necessarily sourced from one standard, but can come from internal and external policies, standards and guidelines. This set of questions is the main instrument to assess the information security related components of a resource, and helps the deployment teams determine what action to take to ensure appropriate controls are implemented. The ISRI is periodically reviewed and updated to capture any new information about the project or to reflect any change in project scope and requirements.

ISR Instrumentation is at the core of the evaluating methodology. It is in this step where the information security and privacy assessment is performed. To that end, there are two steps for preparing an ISRI :

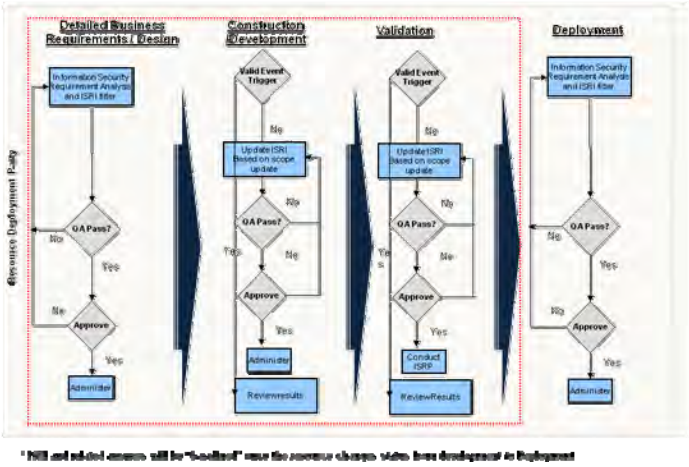
Validating the Instrument – As mentioned above, the key challenge in ISRI is the amount of subjectivity injected in the assessment "Checklists." Upon examination, building these checklists rely uniquely on singular or group knowledge of experts in information security and privacy. The key components of this model are to use a measurement instrument (e.g. survey questionnaire) built with a collaborative effort by information security experts based on field experience, best industry practices and guidelines published by a recognized information security body. The assessment provides a snapshot view of an organization's information security and privacy posture and its supporting infrastructure. However, these instruments are a set of non-scientifically generated survey questions with a binary (yes/no) scale that are mostly compliance centric. Often the problem with these types of scales is that they are highly subjective, produce inconsistent results and the data cannot be used for inferential analysis due to the way they are constructed, administered and the lack of a common risk rating methodology.

Validating these instruments requires either a scientifically reliable method of collaboration or if it is preferable to use a subjective method, then a proven one should be used in a structured manner. One method that can be recommended is using a survey or a process like Delphi to communicate and validate the instrumentation. In either case, it is essential to clearly define the variables that need to be measured and reduce the amount of dependencies among these variables.

Scope Filtering – This step defines the scope of the instrumentation questions administered for a particular resource. The filtering criterion is based on a targeted set of Information Security Questions (ISQ) that acts as an entry point to the ISR Process and is comprised of a set of event triggers. For example, one important event trigger can be a resource's inherent risk determination that will define the control domains for the ISRI and/or automated set of scans that need to be performed. When an ISRI is required, the deployment party must complete the first ISRI filtering criterion with support from the Information Security Officers (ISO) and other project team members. For example if the risk determination of a business application is "High" a scope of the control domains must be identified. Once this step is completed, the assessment rule may include the entire control domain from a validated instrument that will be used for the assessment. On the other hand, if the risk determination is "Low," a reduced version or an existing version of the assessment can be used in lieu. In any case, to reduce the dependency on standards, a static list of control domains must be defined and instrumentation questions can be built around them. An example set of instrumentation questions may encompass the following IS control domain areas:

1. Identification & Authentication
2. Authorization and Access Control
3. Data Confidentiality & Data Integrity
4. Audit Logs
5. Information Security Administration
6. Non-Repudiation
7. System Security & Availability
8. Network Architecture & Perimeter Security
9. Web Application
10. Database Access
11. Web Secure Coding
12. Mobile Guideline Assessment
13. Process Validation
14. General Process Controls
15. Standard Build and Default Configuration

16. Vulnerability Assessment
17. Data Protection & Retention, Log Review
18. Third Party
19. Systems Development & Maintenance
20. Developer Access to Production/ or UAT
21. Change Control Processes
22. Capacity Management



ISR Checkpoints
This is defined as a logical point in time where the deployment parties ensure that ISR events have been treated, changes in the scope of ISRI are addressed, and responses are validated regardless of the SDLC methodology used.

ISR Assessment Optimization in Leverage
This step provides the ability to leverage already available assessments for resources that can be related in a pre-specified one-dimensional tree-like graph. For simplicity, this step can take as its scope a parent/child resource relationship and may leverage an existing assessment with the objective of reducing amount of assessment, deviations from different methodologies and time of assessment. This again will reduce the amount of trickle down changes to the ISIR once policies or standards change. With that in mind, we identify the following three relationships that must be addressed for this optimization and leverage effort:

Leveraging Parent/Child Relationship – If a resource is identified as being a child resource and the parent resource has been assessed, then the entire ISRI can be leveraged for that resource.

Leveraging Other Available Assessments – Resources may identify relationships or dependency to other resources or services (e.g. Infrastructure Components, Infrastructure Service or Other Applications). Leveraging a resource assessment may be done for each question in the ISRI after the relationship has been established. The assessor, with the help of the information owner and deployment party, is responsible for making that decision and assessing whether any issue risks related to the leveraged resources are acceptable or may have other compensating controls that may reduce that risk. Once such a dependency is identified, a notification network must be engaged to alert users of the associated deficiencies. Leveraging completed and current assessments will benefit the efficiency of the process and will reduce the rework efforts when standards change.

Leveraging Previously Completed ISRI Versions – A resource undergoing an ISR may leverage previously completed and approved versions of an ISRI. An ISRI baseline version is created when the resource moves into a final deployment stage. Each time a resource moves into this stage, the previous baseline is replaced by the latest ISRI. A baseline provides the person completing an ISRI subsequently, the ability to leverage the responses in the baseline version. Based on their judgment, they could either accept the responses in the baseline version, or provide a different response. This again reduces the efforts of doing a complete gap analysis against standards every time a resource is required to be assessed.

Conclusion and Future Works

This article provides a proposal for increasing the efficiency of IS&P assessment to include it as part of the SDLC process, while reducing the dependency on standards as a check list, and the associated overhead. Other parts of the process were not discussed here and include the modeling efforts to define risk rating methodologies, variable definition and independence when measuring control deficiencies raised and methodologies to capture, communicate and close corrective actions relating to highlighted control deficiencies. Another area of research is in defining a technology framework (e.g. XML) for transmitting and receiving data across loosely coupled/federated systems that are built to handle various processes.

The Need for Web Standards in Financial Services Industry

J. Alan Bird, Global Business Development Leader, W3C

The Financial Services Industry is one of the most competitive in the world. This competitiveness has driven most organizations to drive key solutions into their ecosystems using internal "standards" while leveraging various technologies. This has resulted in many companies having very robust systems that are great in isolation but not designed or implemented to work in a shared technology environment. With the recent advances in the standards that make up the Web, and that are coordinated by the World Wide Web Consortium (W3C), there is value to be gained by the companies in the Financial Services Industry in adoption of these standards. Implementation of these standards as well as the other standards in place for the industry will result in better solutions for all three key stakeholders in the Industry: Regulation, Company Representatives and Customers. Let's look at each of these in more detail.

Regulation Reporting

In 2009 W3C and XBLR International held a Workshop to discuss what work needs to be undertaken by the standards community to make regulation-defined reporting easier to accomplish. While no tangible work efforts surfaced for W3C out of that work there was one key solution that was identified – adoption of Semantic Web technologies. It was viewed that in the data-rich environment of Financial Services adoption of these technologies would streamline the reporting process by making the data more accessible and easier to disseminate.

In the two years since that Workshop there have been many companies in the industry adopting the Semantic Web but there is still room for collaboration to define a common ontology for Financial Services. The idea that the Semantic Web is an abstraction layer over existing data sources along with being able to express richer semantics than is currently possible in XBRL was voiced in that Workshop and that notion is still valid today and warrants deeper discussion among the various companies in the Financial Services Industry. W3C is prepared to work with the industry to provide a vendor-neutral, royalty-free environment for these discussions.

Company Representative Solutions

The primary live customer point of contact for most Financial Services organizations is their Customer Services Representative organization. This is a highly valued part of the organization and they need to have tools available to them to be quickly responsive to customers while on the phone as well as having robust tools that allow them to do in-depth research and analysis for customers. Most Financial Services organizations have significant investments in the data they maintain about their assets and the markets they serve. The challenge for the Financial Services representatives is to efficiently search their companies data rich repositories to get the information they need to answer a specific customer inquiry. Once this has been completed they then need to augment that research with information from other organizations. Today the quality of the information they are able to obtain is dependent on their ability to do the research using standard search engines and knowing which sources can be trusted. These work efforts could be greatly enhanced by the use of Semantic Web technologies.

Financial Services organizations need to aggressively start turning their data into Open Linked Data. This requires making sure the data is available for query and is tagged so that relationships between the various data elements can be surfaced. Once this effort is done then the resulting research from

Financial Services personnel will be more robust and complete. This should also increase the efficiency of these key resources as the information will become more obvious to them in their work. The other issue that needs to be addressed is ensuring the validity of the data being used. There is a new body of work being done by W3C around standardizing the Provenance of Web resources. The Financial Services industry has a view on this that would greatly enhance the overall work being done and their participation in this dialogue would be beneficial to the industry as a whole. While being responsive to Regulators and having easy-to-use internal systems is important, the major goal of any Financial Services organization should be to provide as rich of an experience as possible to their customers.

Customer Facing Systems

Customer loyalty and satisfaction are key drivers for the Financial Services industry. In today's environment the average consumer of Financial Services has many options on who to work with and changing from one firm to another doesn't involve a significant amount of work on the part of the consumer. In order to reduce customer turnover many Financial Services organizations are investing significant amounts of money to develop, deploy and evolve their customer facing solutions.

While most customers are able to meet their basic query functions via the phone-based solutions that have been deployed, many are looking to have a Web based experience for more detailed review of their accounts and want to be able to take action from these same systems. Once they are on the Web and looking at the Financial Services website they want to be able to do research and analysis of the various holdings they have as well. Additionally they want to be able to research new investment opportunities and potentially execute their transactions from these same Web based tools.

To provide their customers the most robust experience in their research efforts Financial Services organizations need to offer a comprehensive set of tools. These include not only their proprietary market and industry research databases but also the information provided by other Industry organizations like Morningstar. This would be better and more simply achieved by using the Semantic Web standards developed by the World Wide Web Consortium. Once the Financial Services Industry embraces Open Linked Data the ability to do in-depth analysis on any given stock, fund or company will be greatly enhanced.

The customer could start by looking at his portfolio. If one of his holdings is an active link then he can drill down on that link which will generally be the Financial Services organization's analysis of that asset. Within that analysis should be active links pointing to other content about the asset. These may be links to outside reports about the asset company, reviews of the assets activities by other firms, reports from the various regulatory organizations about the asset, etc. This should then be complemented by a complete set of reporting tools that provide rich content in an easy to read format. Providing this level of analysis from within the Financial Services systems increases the value the customer places on using the system as a primary tool and thereby increases the customer's loyalty to the Financial Services organization.

These scenarios have been complicated in recent years by the evolution of the devices that customers want to use to access these systems. The default platform for most customer facing solutions is the desktop or laptop. Many customers, however, are moving to a tablet as their primary device and they want the same services available on that platform that they have historically accessed on their desktop or laptop. This is further complicated by the usage of smartphones and the desire to have full access to their financial services via that device. Without the adoption of Web

Standards like HTML5, CSS and SVG the resources required to offer the systems on this variety of devices is greatly complicated.

The W3C has had a Mobile Web Initiative for over 5 years and that initiative has produced significant enhancements to these and other standards. The goal of this work is to allow organizations to write once, deploy many. This results in a direct savings for the Financial Services organization because they only have to develop and deploy one version of the application instead of specific versions for specific platforms.

Summary

The Financial Services industry is one of the most data-rich environments on the Web today, however access to this data is often inhibited by the lack of adoption of standards by the industry. Adoption of Semantic Web best practices and technologies would greatly enhance the solutions that are available to both the industry personnel and the customers of the industry. Adoption of the standards around how websites look and respond would enhance the overall customer experience which would increase customer loyalty. W3C is the place where companies are working together to drive these standards and the voice of the Financial Services organizations needs to be added to this dialogue.

J. Alan Bird

Mr. Bird is the Global Business Development Leader for the World Wide Web Consortium (W3C). Prior to joining W3C Mr. Bird was a Financial Services Representative with his Series 6, Series 63 and MA Insurance Licenses. Prior to that Mr. Bird has worked for various leaders in the Software Industry.