



A Security Enterprise Architecture for Healthcare (SEAFH)

By Tom Tuduc

Introduction

To comply with HIPAA and to provide best services under limited resources and time, healthcare organizations often have to make decisions that involve conflicting objectives. For example, what is the ROI of an identity management system that requires significant staff time and resources to integrate with directory servers and domain authentication systems? How should healthcare organizations perform due diligence, risk and quantitative ROI assessments, create policies, processes, and best practices? This article employs a framework and methodology that draws from IT best practices to help all healthcare organizations.

Why is HIPAA Security Hard to Deal With?

HIPAA security rules are flexible within an acceptable range of risk. Health care organizations have to determine what is the acceptable range of risk they can tolerate to guard the confidentiality, integrity, and availability of Protected Health Information (PHI). Specifically, organizations need to determine how to implement security controls and policies based on their own risk assessments. The more complex the organization and its information infrastructure, the more complex the risk assessment and its consequences, primarily analysis, control, and monitoring.

HIPAA brings PHI information risk management to the same level of compliance as infectious disease control, ethical practices, and billing fraud. Legal advisors recommend that security should be treated at a CXO level in an organization¹.

Organizations in the HIPAA space are concerned about how to comply with the security rules because they do not provide clear compliance directions. Each organization, to their discretion, decides on how much to spend and what problem to address. For example, if a healthcare organization does not use e-mail encryption, then security policies or risk analysis in this area may not be needed. However, if e-mail encryption is used, there are specific controls and guidelines to follow.

HIPAA compliance and HIPAA security ROI is a complex arena of several bodies of knowledge. Most security professionals do not speak financial ROI and risk management languages. Most enterprise architects are just beginning to use security vocabularies. Most policy makers (chief privacy officers and lawyers) and financial analysts are not well-versed in the technical level of IT security. The SEAFH framework will help collaborations and communication by providing a blueprint, perspectives and the larger picture.

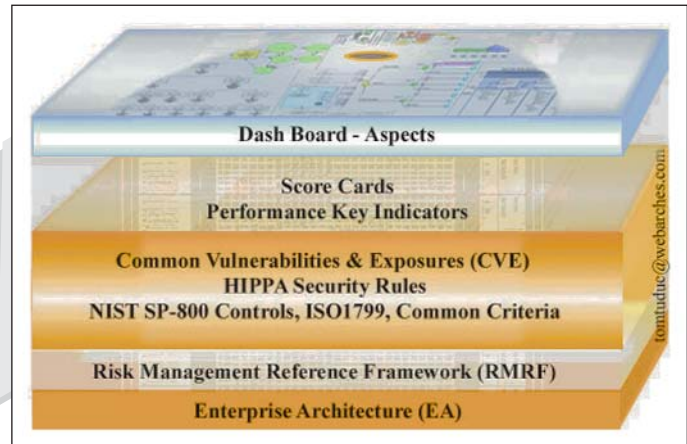


Figure 1a: Security Enterprise Architecture for Healthcare (SEAFH) Framework

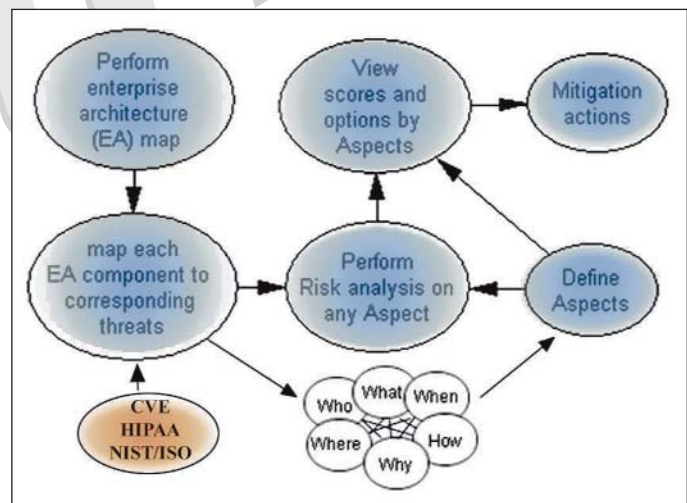


Figure 1b: Dynamic snapshot of SEAFH Framework

SEAFH: An Overview

Security threats are moving targets that security strategies must consider. New technology and security vulnerabilities limit the effectiveness of any strategy. A particular strategy may become obsolete by the time it is implemented. To be in the best position to deal with security and HIPAA compliance, organizations must master three areas of knowledge: HIPAA, IT security and ROI of specific security controls. Consider these three concepts:

1. Uncertainties and Risk Management.

2. Enterprise Architecture (EA)
3. Balanced Score Card (BSC)

Until recently, the cost of computing and lack of tools have inhibited methodologies and processes for integrating these three bodies of knowledge.

Why SEAFH?

Historically, healthcare lags the financial industry in risk management. However, HIPAA regulations may change this pattern. While rigorous and quantitative risk management in security and security ROI is still in its infancy across industries, the financial industry leads the pack in security risk ROI. In a healthcare panel facilitated by the Tunitas group at the RSA 2004 conference, a healthcare CIO/CSO called for a quantitative risk management plan similar to Bank One's presentation in the previous day². Healthcare security risk management and ROI do not have a reference implementation, standardized methodology, and known best practices.

A security risk methodology for healthcare differs from the financial industry in the "who, what, when and where," but not the "how." One of the components of SEAFH is the BSC with Performance Key Indicator. It proves its success across all vertical industries. Specific quantitative risk management with business ROI in healthcare is often found in BSC implementations. In addition, risk management and ROI using Bayesian decision analysis are numerous in healthcare and pharmaceutical product introduction, drug benefits, and IT functionality ROI. Security ROI, however, has not had much focus.

SEAFH framework is not a theory or a model. It is a methodology combining industry-proven practices for over two decades: EA, BSC and quantitative risk management. Hospitals have been using various forms of quality improvement methodologies including Six Sigma, Business Process Management, and more recently, BSC. Security processes, policies and specific mitigations of networks, appliances and applications are beginning to gain business attention, largely due to regulations.

Components of SEAFH are well understood and successfully implemented in over a hundred healthcare organizations. Large hospitals have started using EA tools to help document the "who, what, when, where, why" of all hospital functions. Kidhealth and Dupont Hospital used a comprehensive EA assessment to help them integrate and improve their IT functionalities including security³. There are many examples of BSCs in clinical environments (see BSC section).

SEAFH Components

The following sections give an overview of the three mentioned bodies of knowledge and how they play out in healthcare security.

Uncertainties and Risk Management

Uncertainties are ubiquitous in security tools, their effectiveness, and security ROI. Security technologies including behavior-based intrusion detection systems, statistical-based intrusion detection systems and Spam filters⁴ are based on quantitative analysis such as Bayesian probability and statistics. The next wave of security technology in intrusion prevention systems will rely even more heavily on quantitative analysis and Bayesian probability. For example, unknown intruders with unknown signatures require various expert judgments in infrastructure technologies including networking, voice over IP, as well as industry specific applications and systems. "Trustworthy Refinement through Intrusion-Aware Design" is an example of a next-generation project using Bayesian net and influence diagrams at Carnegie Mellon Institute⁵.

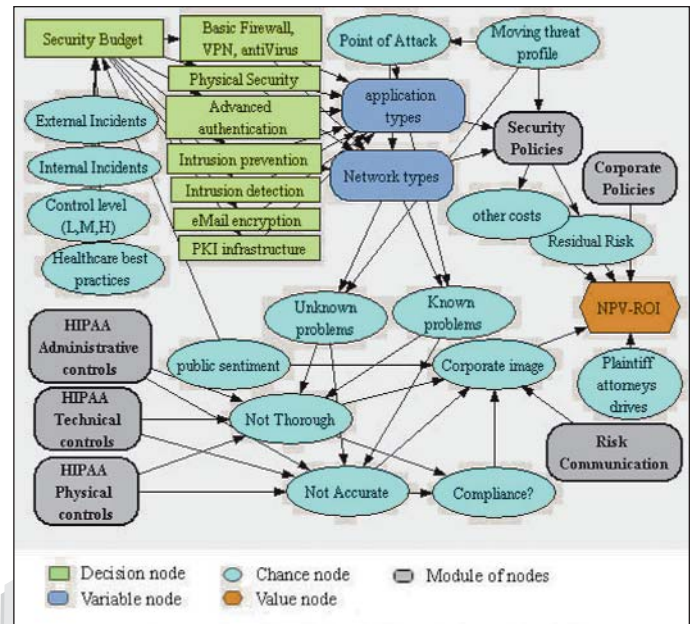


Figure 2: Snapshot of a Security Budget Aspect modeled in Analytica

On the business side, quantitative security ROI and quantitative risk management gain much visibility as security regulations are coming in effect. For example, Bank One employs probability trees to minimize the rate systems get hacked and factors preceding successful attack². Likewise, Deutsche Bank deploys an information security risk metrics systems using ROI, risk indicator, cost avoidance and cost reduction⁶.

In calculating ROI, quantitative analysis is an effective tool for vendor selection. Other quantitative analysis include policy analysis, policy portfolio, risk assessment, and risk analysis. ROI calculations include:

1. For what size of organization and how should access control be used?
2. How complex an organization, its processes, and computing entities when it becomes cost-inhibitive to maintain and monitor the access control rules?
3. When to use access control, or the surveillance of personnel, and when to choose accountability, or the surveillance of data?
4. What is the optimal number of network scans for vulnerabilities, internal and external, per year, as scanning means loss of productivity in addition to costs?

In security ROI and budgeting it is often believed that the lack of a serious breach in the previous fiscal year means security has been over-budgeted. Here a risk management framework can provide technical security personnel a financial yardstick for much-needed security budgets.

Where there are no security statistics for every hardware, appliance and software, organizations employing quantitative analysis should start with general statistics (CSI/FBI Computer Crime and Security Survey, <http://www.securitystats.com/>, @stakes.com) and collect data by monitoring all traffic and employing honeypots

Enterprise Architecture (EA)

EA is the knowledge of the current state of the organization. In business process management, this is the AS-IS state of the organization in terms of its assets, processes, personnel, data, and other computing entities. Knowing the AS-ISs enable organizations to know possible TO-BE architectures.

In dealing with the AS-IS and TO-BE architectures, organizations can employ EA documents to make the transition painless. To reduce unauthorized access to data and comply with HIPAA while enabling doctors to access patient data in every exam room, Northwestern Memorial Physicians Group's new architecture employs PC blades. These PC blades are centrally located in a back room while minimal user interfaces are in the exam rooms. In addition, doctors wear a radio-frequency identification tag to activate the terminals when they enter the room. In this example, the patients get the same services (customer functions) while some computing entities and processes got changed. An EA document can show the difference between the two architectures and which uncertainty was reduced or eliminated. EA is the map of the computing entities and processes of an organization.

Balanced Scorecard (BSC)

BSC is a method for measuring progress and managing milestones. Taking concepts from Six Sigma, Total Quality Management and Continuous Quality Management, BSC provides clear connections of cause and effect in business performance. Viewing information security from a quality perspective puts security policies, assessment, prevention, and monitoring right in the BSC cross hair.

Examples of healthcare organizations employing BSC include Aurora Health Care—Wisconsin's largest private employer, Hutchinson Area Health Care, Ontario Hospital, and the American Red Cross. Hundreds of other healthcare organizations are using BSC to improve clinical care and hospital management.

SEAFH: A Closer Look

SEAFH is a methodology that optimizes resources to produce the best security strategy for healthcare, including healthcare IT security ROI and IT security processes. SEAFH consists of the following main components:

1. Dashboard
2. Score card—Performance Key Indicator (PKI)
3. Enterprise Architecture (EA)
4. Risk Management Reference Framework (RMRF)
5. Common Vulnerabilities and Exposures (CVE)
6. HIPAA security rules
7. Security Standards and Controls

While EA models the flow and components of security information, RMRF models the uncertainties of the information as well as the uncertain relationships between the information (the probability of a port-scan attack, the probability of applications opening and closing ports).

Complexity is the main enemy of security. SEAFH transforms complexity into manageable components and processes. First SEAFH models all entities. Entities include hardware, software, processes, and personnel. The modeling creates standardized views such as data view, process view, personnel view, geographical view, and time view. More specialized views, using any particular combination of data, process, personnel, location, and time are called aspects.

The SEAFH framework is shown in Figure 1 and 2. While each component is taken from separate bodies of knowledge and can be modeled in parallel, the EA component is often the first component to be modeled in order to give a comprehensive view of all involved entities of an organization. Figure 3 shows a snapshot of an aspect modeled using Analytica[®], a risk modeling tool.

While SEAFH incorporates industry best practices to provide a framework, security controls are provided by standards and regulations including HIPAA security rules, NIST SP 800 series, ISO1799, and Common

	What (data)	How (function)*	Where (infrastructure)	Who (people)	When (time)	Why (motivation)
Context	List of things	List of processes	List of locations	List of organizations	List of events	List of business goals
Enterprise model	Semantic model	Business process model	Logistics network	Workflow model	Master schedule	Business Plan
System model	Logical data model	Application architecture	Distribution model	Human interface model	Process schedule	Business rule model
Architectural model	Data Design	Software—Hardware design	System Architecture	Presentation architecture	Control structure	Business rule design
Technical Detail	Data definition	i.e. Programs	i.e. networks	i.e. access control—security	Time definition	Rule specification

* Function: medical, clinical, billing, pharmacy, emergency, etc.

Figure 3: Enterprise Architecture (Adopted from Zachman Framework)

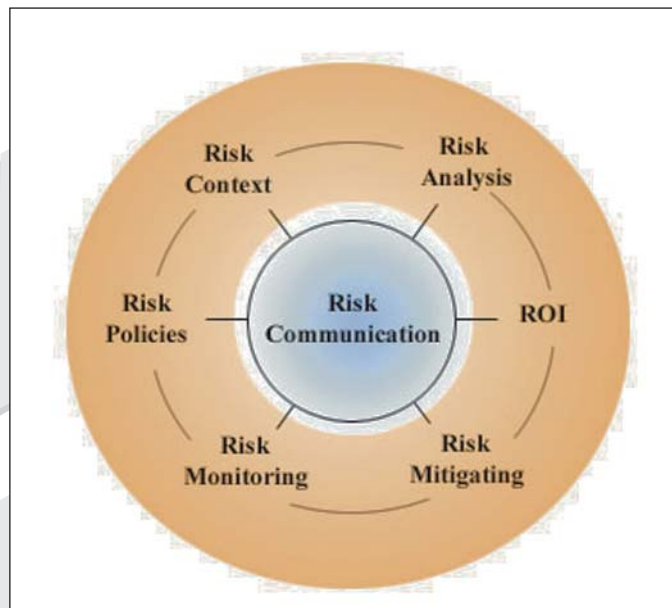


Figure 4: Risk Management Reference Framework (RMRF)

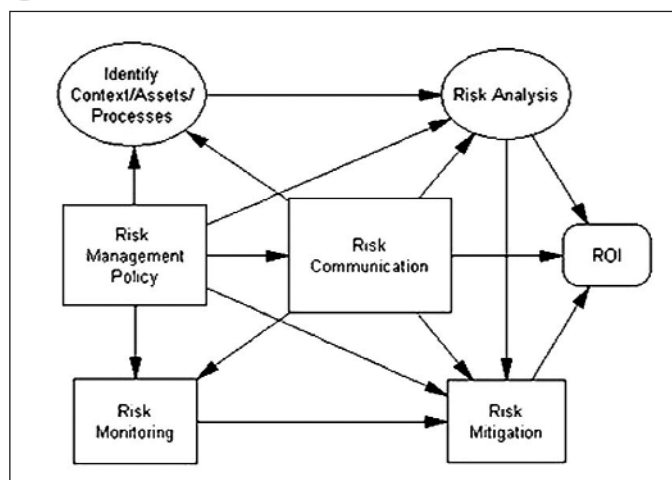


Figure 5: Dynamic RMRF modeled by Analytica Decision Analysis

Criteria. The BSC and risk management framework components enable ROI planning and monitoring and improvement of security processes.

The following sections give a closer look into some of the components of this methodology.

Enterprise Architecture (EA) Documents

This consists of:

1. Tangible assets: hardware, software, equipments, appliances, networks, devices.
2. Intangible assets including data, automated processes, and non-automated processes (processes are examples of the "hows")
3. Strategic assets: people, business strategies, business rules, corporate risk and goals.

An EA document can be a few pages or hundreds of pages depending on the depth and complexities of the organization. In either case, it provides the six dimensions views: what, how, where, who, when and why (Figure 4). These views can be used for analysis (whether to implement access control, data surveillance, behavioral based intrusion-detection, patch management, or forensics).

Additional Resources:

- United States Department of Health & Human Services, 2/20/03 HIPAA Health Insurance Reform.
 - Security Standards Final Rule. <http://aspe.hhs.gov/admsimp/FINAL/FR03-8334.pdf>
 - Administrative Simplification in the Health Care Industry. <http://aspe.hhs.gov/admsimp/index.shtml>
- Visumhealthcare. "What is Balanced Scorecard – Health Care Performance Management" http://www.visumhealthcare.com/index1.php?info=hpm_bc_bs
- Arveson, Paul. "The Convergence of Strategy, Performance and Enterprise Architecture in the US Federal Government." <http://www.balancedscorecard.org/bscit/prm.html>
- The ISSA Journal,
 - http://www.issa.org/cgi/journallibrary.cgi?download=2003_May/J0305001.pdf
 - http://www.issa.org/cgi/journallibrary.cgi?download=2003_April/200304JL.pdf
- Robinson, Brian. "Enterprise Architecture Modeling Emerges as Key Tool for Improving Readiness." <http://www.fcw.com/supplements/homeland/2003/sup4/hom-arch-12-01-03.asp>

Risk Management Reference Framework (RMRF)

RMRF consists of risk analysis, including qualitative and quantitative, risk mitigation, risk monitoring, and risk communication (Figure 4 and 5). Primary risk analysis techniques include Monte Carlo, decision analysis/influence diagram, and secondary techniques, including game theory and systems theory. Security system behavior can be simulated using Monte Carlo, while best decisions can be obtained using expected utility, value of information and control, etc.⁹

ROI is defined as ratio of savings to cost. Costs include time and human and computing resources. Savings include cost avoidance and cost reduction (Hall 1998).

RMRF maps enterprise entities (who, what, when, where, why, and how) to each security vulnerability and threat. Each of the asset entities can have attributes such as exposure factor, single loss expectancy, annualized rate of occurrence, and annualized loss expectancy (as defined by Shon Harris in CISSP...)

RMRF can employ the BSC component that shows risk indexes of aspects at any given time with respect to up-to-date threats. Risk calculations such as trends, forecasts, and mitigation for aspects can include tangible, intangible, and strategic assets.

Aspects

RMRF can be superimposed on top of IT security processes and EA documents as a guide to produce documents and reports. RMRF uses aspects as means for user interfaces and risk ranking. RMRF provides a methodology to analyze, mitigate and manage known, unknown and unknowable security vulnerability and threats by ranking aspects by a risk index. Aspects are inputs to the RMRF and comprise unique sets of related objects/entities describing specific functions. For example, accounting functions of a company have sets of objects/data/personnel uniquely describing those functions.

Balanced Score Card (BSC)

The balanced scorecard is a management and measurement system that enables organizations to articulate their goals and strategy and map them to processes and indicators (Balancedscorecard.org). Healthcare performance applications are numerous (Visumhealthcare.com).


A typical BSC implementation includes four perspectives:

1. Financial Value

2. Business Process and Operation
3. Customer View Points
4. Continuous Improvement

Security failure can be viewed as quality failure and can be measured and controlled using BSC. A BSC adaptation for security contains a similar four perspectives. Here the financial value perspective articulates the business value of security initiatives (how security applications enable business strategies).¹¹

Conclusion

By piecing together industry best practices, HIPAA regulations and industry standard control procedures, healthcare organizations can effectively manage the complexity of enterprise security issues, assessments, policies, monitoring and communication. By employing a reference framework, organizations can reuse bodies of knowledge available in enterprise architecture, risk and decision analysis, and BSCs. This reuse and integration is the key to bring order to a chaotic world of security threats, vulnerabilities and exploitations. 

Tom Tuduc is a consultant in risk management, security analytics and enterprise integration/Web services. He worked at IBM and Boeing Labs and developed software at Interactive Home Systems (Corbis). He served on OASIS eGovernment and eProcurement Technical Committees and participated in WS-Security committee 2002-2003.

¹ Tunitas Group. "HIPAA Security Rule." http://www.tunitas.com/presentations/HIPAA_Security_UCSF.pdf

² School, Albert. "Information Security Threat Modeling: A Risk-Based Approach." Bank One Corporation, RSA Conference 2/24/2004. San Francisco, CA.

³ Kidhealth and Dupont. (http://www.vector.com/casestudies/PDFs/Case_Study_Nemours2.pdf)

⁴ Graham, Paul. "Better Bayesian Filtering." <http://www.paulgraham.com/better.html>

⁵ Ellison, R.J., and Moore, A. P. 2003. "TRIAD - Trustworthy Refinement through Intrusion-Aware Design." TECHNICAL REPORT CMU/SEI-2003-TR-002. ESC-TR-2003-002 Coordination Center. Software Engineering Institute. Carnegie Mellon University/ <http://www.cert.org/archive/pdf/triad.pdf>

⁶ Duliba, Katherine. "Information Security Risk Metrics: How to Quantitatively Assess Applications." Deutsche Bank. RSA Conference 2/24/2004. San Francisco, CA.

⁷ Geer, Dan. "The Shrinking Perimeter: Making the Case for Data-Level Risk Management." <http://www.verdasys.com/download/download.php?file=ShrinkPerim.pdf>

⁸ Lumina Decision Systems. "Influence Diagrams." <http://www.lumina.com/software/influencediagrams.html>

⁹ Tuduc, Tom. "Homeland Security Quantitative Risk Analysis." *The ISSA Journal*, January 2004.

¹⁰ Tuduc, Tom. "Security Architecture Risk Reference Framework." <http://www.webarches.com/EASecurityRiskManagement.htm>

¹¹ Giga Information Group, Chief Security Officer Online, "Aligning Security with the Business: The 'Balanced Scorecard.'" <http://www.csonline.com/analyst/report816.html>