GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Leadership Essentials for Managers (Cybersecurity Leadership 512)"
at http://www.giac.org/registration/gslc

A Plan for How to Get There and What to Do When You Arrive: Practical Advice on Establishing a Security Information Management Program within Healthcare

GIAC (GLSC) Gold Certification

Author: Barbara Filkins, filkins@impulse.net
Advisor: Richard Carbone
Accepted: January 16, 2014

Template Version September 2014

Abstract

Security, practiced correctly, is a pervasive discipline literally touching each aspect of an organization's systems, workflows, and practices. Ideally, it should be realized as embedded in the day-to-day activities of the organization, not a disruptive practice "bolted on" as an afterthought. Risk assessment and management needs to be ongoing – when changes occur in the environment, when key personnel leave. Incident response needs to focus on proactive practices to try to flag a potential incident before it becomes an actual breach. For these reasons as well as regulatory compliance, an organization should establish an information security management program as opposed to piecemeal processes that band-aid gaps but never treat the underlying illness or wound.

Your project is approved. How do you to accomplish what you need to, how do you get there, and how do you prove that you accomplished what you set out to achieve? This paper will outline actionable steps that address these questions, providing tools and templates, where practical. A representative use case, based on the creation of such a program for a public health care entity with a workforce of over 500 users is used to illustrate the concepts in this paper.

filkins@impulse.net

© 2015 The SANS Institute Author retains full rights.

1. Introduction

Health care, as an industry, is stressed from all sides as it tries to improve its privacy and security posture in the age of the electronic health record (EHR). The sector in general suffers from increased regulatory compliance, continued uncertainty over the nature of audits and sanctions, greater demand for appropriately trained staff, and "heightened recognition that health care information and health care identity are worth money—and that the bad guys can and will launch cyber-attacks against vulnerable health care networks" (Filkins, 2014).

Approaches to information privacy and security are needed which address these problems while still allowing the health care profession to meet its primary mission – providing care to patients. This is the challenge faced by the GIAC Behavioral Health Agency, run by a local County government.

The Director of Operations commissioned a gap/risk assessment report around the Agency's information security posture. The final document contains 77 distinct recommendations of varying priority and complexity – all the way from developing an enterprise security architecture to completing a handful of policies still in draft. There is a huge flurry of activity – several committees have been formed, a policy writer hired, new network assessment tools obtained – and yet nothing is really getting done.

The Agency's Chief Security Officer (CSO) has selected you, based on your credentials and reputation, to lead a coordinated effort for implementing security compliance in the Agency. You have made your initial presentation to the management team and now have their backing, adequate funding based on cost/benefit justification, and committed resources for twelve months. The challenge you face is – how do you actually make something happen, something that will be worthwhile, something that might actually ensure a lasting culture of effective privacy and security (as well as regulatory compliance) within the Agency?

You are about to embark on a journey – you know your destination (even if it is an interim one) but you need a charted course (with waypoints to keep you on course) and a flight plan. This paper is intended to help you identify and create both.

filkins@impulse.net

© 2015 The SANS Institute Author retains full rights.

2. Understanding the Organization and Its Needs

Even before thinking about your approach, you need to understand the organization. As you reviewed the assessment report, you gained an understanding of the Agency mission and the orientation of its culture to patient privacy and information security.

The GIAC Agency is a behavioral health provider – the clinical and social worker staff treat short-term mental illness (i.e., depression) as well as substance abuse patients. There are about 500 users, including 200 directly contracted providers, most of whom use the Agency's information systems and some of whom have their own.

September 23, 2013 marked the deadline for compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Omnibus Rule, establishing an updated floor for privacy and security in the United States health care industry (Mont, 2013). The Agency is required to be compliant with all aspect of the Omnibus Rule, of which the HIPAA Privacy and Security Rules are a part.

As a behavioral health organization, the Agency is subject to additional federal regulations that reach beyond HIPAA privacy and security requirements such as 42 C.F.R. for substance abuse and 38 C.F.R. for veterans. The exchange of personally identifiable information (PII) as well as electronic protected health information (ePHI) with the forensic and school systems in the County invoke other legal considerations. A preemption analysis shows where State regulations more stringent than HIPAA are in effect (Pritts, 2003).

The Agency workforce has a strong sense of mission to its clients, often at the expense of privacy and security. Most incidents are due to trying to get the job done and involve as much mishandling of paper records as well as electronic information. While there is mandatory training on the HIPAA Security Rule, there is little or no security awareness training and definitely no education as to security "best practices" for Agency end-users.

The Agency's technical infrastructure is extremely solid. Information systems are centralized at the County data center and the County network provides robust connectivity. End-user support for the electronic health record and the practice management systems are available from 6 am to 6 pm, Monday through Friday and 6 to noon on Saturday. Lack of system availability is not a problem as most users can easily move to downtime procedures on paper and catch up later between client sessions. The system(s) generally have never been down for more

filkins@impulse.net

© 2015 The SANS Institute Author retains full rights.

than an hour at a time. There are currently no requirements for 24 x 7 availability, as would be required to support inpatient facilities.

Organizationally, information technology (IT) responsibilities are split. The local government of which this Agency is a part, manages the network infrastructure and its perimeter controls. The Agency IT department maintains the servers, the workstations, and the main information systems – the EHR, the billing systems, and various links to required State reporting sites. The clinical staff is highly mobile with Agency-issued laptops and personal smart phones (i.e., BYOD). The use of tablets is still small but growing.

The Agency has flexibility in its approach to implementing solutions to the standard and implementation specifications of the HIPAA Security Rule. According to section §164.306, it "may use any security measures that allow [it] to reasonably and appropriately implement the standards and implementation specifications" of the Rule (HIPAA, 2014). The recommendations you will provide will not necessarily require the Agency purchase any additional hardware, software or services – just that the course of action needs to make sense in terms of Agency size, complexity, and capabilities, taking into consideration the following business drivers:

1. Sensitivity of the electronic data involved (i.e., mental health, substance abuse)
2. The probability and criticality of potential risks to this information
3. Current and planned resources (i.e., staff available for operations, maintenance, and training) and capabilities (i.e., technical infrastructure including network, software, hardware)
4. Effectiveness of current controls (e.g., processes, policies and procedures (P&P), tools)
5. Budget and cost considerations (i.e., cost-benefit analysis).

3. Justifying a Program Approach

According to the PMBOK Guide, a program is "defined as a group of related projects, subprograms, and program activities managed in a coordinated way to obtain benefits not available from managing them individually. Programs may include elements of related work outside the scope of the discrete projects in the program. A project may or may not be part of a

© 2015 The SANS Institute Author retains full rights.

program, but a program will always have projects" (Project Management Institute (PMI), 2013, p. 9).

Security practiced correctly is a pervasive discipline, literally touching each aspect of an organization's systems, workflows, and practices, cutting across internal boundaries within an organization. It is often closely bound to other concerns such as privacy, integrity, and availability. It touches people, technology, and the use of technology by people. To be truly effective, it should be holistically managed in a coordinated way as referenced in the PMI definition above. This thought is underscored in the 2003 preamble to Final HIPAA Security Rule, which states that the standards were ordered in such a way "that the ''Security management process'' is listed first under the "Administrative safeguards'' section, as […] this forms the foundation on which all of the other standards depend" (Health Insurance Reform: Security Standards; Final Rule, 2003, p. 8344). The Agency needs to establish an information security management program as opposed to piecemeal projects that band-aid the gaps or risks but never treat the underlying illness or wound.

You have convinced executive management that a "program approach" rather than "remediation projects" is the way to approach the needed improvements to security, both for compliance and for actual protection of Agency assets. Key reasons you cite include:

- Remediation of the identified gaps and existing risks requires a financial investment. Good security is based on many good IT practices, many not specific to security such as change or configuration management. Why not make an investment for the future, one that can improve the financial, operational, and compliance posture of the Agency, by establishing a security program and governance structure that involves all the key stakeholders, including IT?
- Security starts with the Agency workforce. Unless there is a cultural shift in how people think about information security, the Agency will face many of the same problems identified in the assessment report again in twelve months. Why not invest in a training and awareness program that helps build security best practices into the culture of the Agency, into the daily processes used by the workforce to serve clients and patients?
- HIPAA is currently the Agency's main compliance focus. Having an active security management program with a well-established risk management process can send the right

filkins@impulse.net

© 2015 The SANS Institute Author retains full rights.

signals to oversight agencies, such as Office of the National Coordinator (ONC), that the Agency takes security seriously. This may not eliminate fines but it could possibly mitigate them.

4. Prepare for Action: Initiation and Planning

Preparation starts with summarizing significant findings from the assessment report, prioritizing elements of a strategy based on these findings, and developing initial tasks and a twelve month timeline from which a project plan to establish the security management program will be created. Initial activities will be aligned with similar processes defined in the PMI Initiating and Planning Process Groups – developing a program charter, establishing governance planning and defining success criteria and metrics (PMI, 2013, pp. 54-55). You will take these elements and begin to lay the groundwork for success with the key stakeholders.

Next, you select an appropriate information security framework to help shape the Agency's program. An information security framework is "a series of documented processes that are used to define policies and procedures around the implementation and ongoing management of information security controls in an enterprise environment" (Granneman, 2013). A framework essentially provides the set of plans to support the orderly construction of an information security program, similar to blueprints in the construction industry. Well-known examples of frameworks include NIST SP-800, FISMA, Critical Controls, COBIT, ISO 27000, and HIPAA.

You select the HIPAA Security Rule as the basic framework for the Agency as this best supports their regulatory compliance needs. The Rule was written to work in conjunction with the HIPAA Privacy Rule (Health Insurance Reform: Security Standards; Final Rule, 2003, p. 8373). It "operationalizes the protections contained in the Privacy Rule by addressing the technical and non-technical safeguards that organizations [….] must put in place to secure individuals' "electronic protected health information" (e-PHI)" ("Summary of the HIPAA Security Rule," n.d.). It outlines an elegant structure that provides a viable means to both plan and organize the Agency's information security program. Designed to be technology neutral, it is still relevant in today's era of mobile and cloud computing.

filkins@impulse.net

© 2015 The SANS Institute Author retains full rights.

4.1. Define Your Security Governance Model

Governance can mean different things to different organizations. In general, however, governance allows an organization to establish strategic direction and performance parameters (PMI, 2013, p. 14). Information security governance starts with "viewing adequate security as a non-negotiable requirement of being in business," where "adequate" is achieved by balancing an organization's appetite and tolerance for risk with a strategy for how its critical business assets and processes will be protected (Allen, 2005).

A formal governance structure will steer, control, and evaluate the program. Steering involves setting the direction of the program within the Agency by involving key stakeholders to help remove obstacles, manage the critical success factors, and remediate program or benefit-realization shortfalls. Controlling maintains the program direction by involving members of the Agency community to ensure commitment, achievement of results, and proactive resolution of leading indicators of possible failure. Evaluation includes defining and measuring the desired outcomes, benefits, and value against planned and measureable expectations as part of quality and performance management.

Your goal is that security be effective, that it becomes "part of the culture of the organization and guides behavior," and is sustainable (Herzig & Healthcare Information and Management Systems Society, 2010, p. 7). Take the time to develop an effective statement that clearly communicates the common mission of the security management program to all stakeholders. Lay out a progressive set of program performance objectives that maintains the "adequate" balance between risk and protection, yet allows for evolution and change. Make sure that the key activities are defined that will guarantee sustainability.

Three key artifacts support Agency security governance. First, the Charter establishes program goals, performance objectives, and scope, defines the critical factors and completion criteria for success, and outlines program activities and structure at a high level. Appendix B provides an annotated outline used effectively in other engagements.

Next, the Governance Plan serves as a foundation document that defines the key governance activities for the program such as risk management, training and awareness, and change control/configuration management. Some of these processes may already be

filkins@impulse.net

© 2015 The SANS Institute Author retains full rights.

implemented within the Agency but this plan will make them specific to information security. Appendix C contains an annotated outline of a representative Governance Plan.

Finally, establish and document the measures for demonstrating success, a key aspect of governance evaluation. Metrics need to be defined, actual indicator(s) designed that represent each metric, method, and data source determined to acquire each indicator, and the initial target values to be achieved for success established. For example, the Agency may select a metric that states, "How many potential breaches were resolved versus encountered?" The indicator is "# of potential breaches resolved without incident / # potential breaches x 100%." The method and data source will be determined based on the Agency's monitoring procedures and the rules that identify potential breaches. The initial target for success is an indicator of 100%.

4.2. Implement Your Security Organization

Next, you determine how to best leverage the organizational structure of the Agency. Existing resources, culture, and attitude can all be barriers to or enablers of what you are trying to achieve. Who is the executive sponsor or business owner for the information security program? Who are the stakeholders? What is the perception of end-users regarding security? Know the normal communications pathways. Where do the CSO, the Chief Privacy Officer (CPO), and compliance officer report in the organization? Who are the "go to" individuals? You need to examine how decisions within the Agency are made. Who has the authority for compliance? You will need all this knowledge when you start to implement the program governance structure.

Your approved approach calls for establishing a steering committee (SC) to provide executive-level oversight for the program. Defining SC roles and decision-making powers was a significant part of developing the Governance Plan in order to facilitate a clear, unified direction for security within the Agency. In this governance model, the SC is a decision-making as well as advisory body. Issues that cannot be resolved at lower levels are escalated to the SC for final disposition. Voting SC membership is restricted to Agency management but the SC also coordinates with other County management entities.

At the program management level, the plan is to implement a multi-disciplinary team structure that reports to the CSO and represents key stakeholders within the Agency. This approach is taken for two reasons: 1) break down barriers between functional end-users and

© 2015 The SANS Institute Author retains full rights.

security to foster the inclusion of security into the overall Agency culture and 2) foster cooperation between those responsible for IT and those responsible for IT security, despite the natural tendency towards separation of these duties.

The formation of three basic teams is based on the list of common computer security incident response services as outlined in the Handbook for Computer Incident Response Teams (West-Brown, Stikvoort, Kossakowski, & Carnegie-Mellon Univ. Pittsburgh Pa Software Engineering Inst, 2003, p. 24-25).

1) The **Operational Security Team** is responsible for routine protection of the Agency's electronic information, maintaining its security posture through performing 'proactive' services -- the day-to-day activities to guard and improve the organization's data, infrastructure, and business processes before any incident is detected or occurs. The services that this team provides are **proactive**, intended to reduce the number of future incidents that occur and to mitigate their impact and scope when they do.

2) The **Rapid Response Team** is responsible for emergency or priority matters, including incident handling and disaster recovery. The services this team provides are **reactive** in nature, triggered by an event or request that likely will become an incident. This team responds to requests for assistance from compliance, reports from the Agency workforce, and any threats or attacks detected against Agency assets initiated through third-party notification, identified through monitoring logs and automated alerts, or flagged by the Operational Security Team.

3) The **Security Quality Management (QM) Team** is responsible for defining and managing those well-known, established services designed to improve the overall security of an organization. For example, this team leads the Agency security risk assessment process, analyzes findings, and acts on outcomes. The team integrates feedback from routine operations and lessons learned in reacting to incidents, breaches, and cyber-attacks into their analysis. Separation of the QM services from normal and emergency operations allows for independent analysis that does not bear the negative connotation of audit, but can support both immediate and long-term improvement of the Agency's security posture.

filkins@impulse.net

© 2015 The SANS Institute Author retains full rights.

The responsibilities of each team member should align with his or her normal role in the organizational structure to avoid working at cross-purposes to his or her normal job. Figure 1 demonstrates the implementation of the program organization within the current management structure of the Agency.

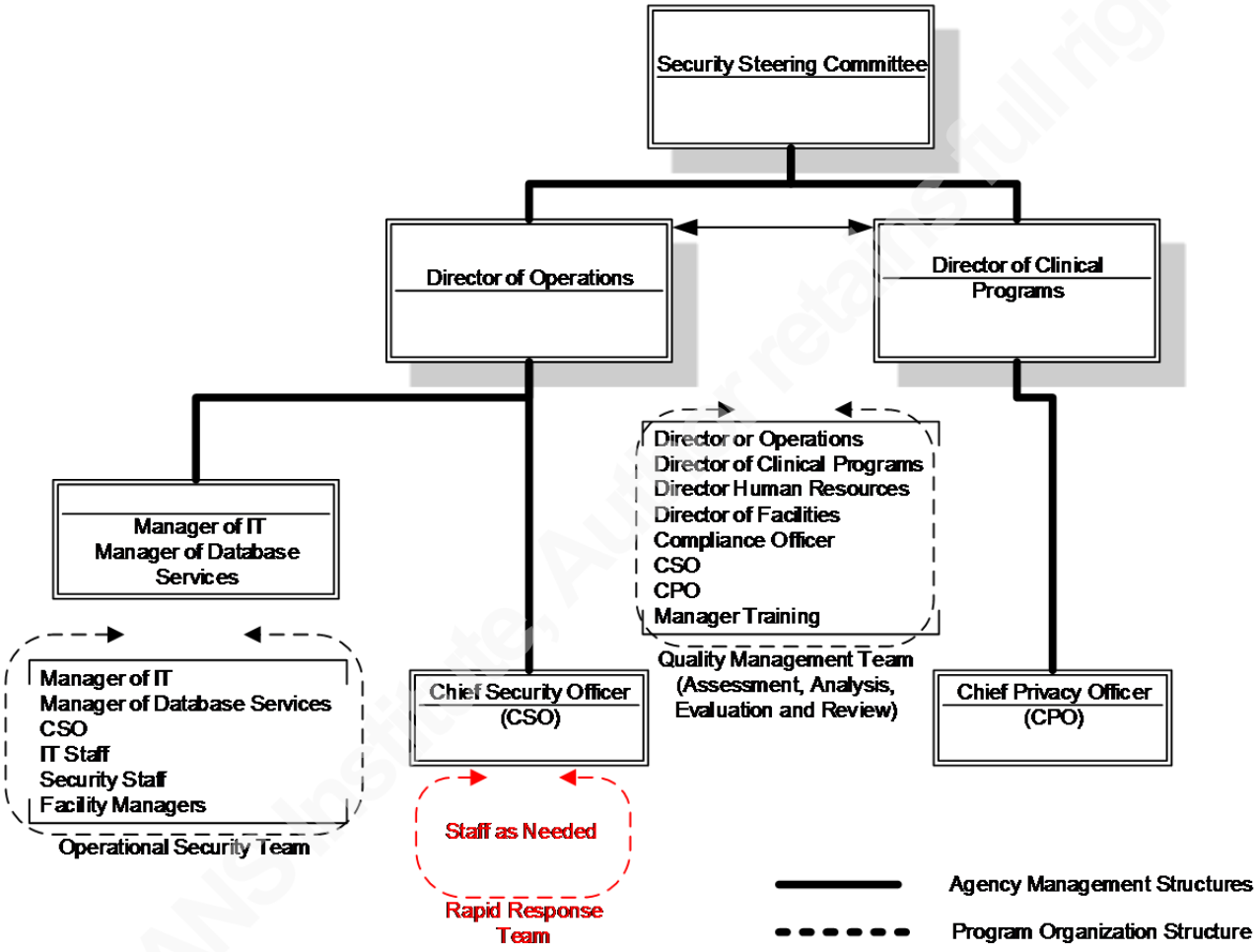

Figure 1: The Agency Security Management Organization

The Agency CSO remains responsible as the main point of contact for all security-related issues and activities needed to maintain the confidentiality, integrity, and availability of Agency information systems, but takes on the role of security program manager, responsible for coordinating and facilitating the activities of the three teams. The CSO works in partnership with the CPO, who in turn reports to the Director of Clinical Programs, and his team.

Table 1 shows the membership of each Security Team for the Agency. As program director, the CSO is a standing member of each team and leads the Rapid Response Team.

filkins@impulse.net

© 2015 The SANS Institute Author retains full rights.

Table 1: Security Team Membership (* = Team Lead)

Functional Area	Role/Responsibility	Team Membership			Title
		Ops	Rapid	QM	
Information Management, Information Technology	Manage privacy and security for data and information, applications, infrastructure. Provide end-user support.	X* X* X	X X X		Manager of IT Manager of Database Services Manager of Charts & Records IT/Security Staff
HR/Training	Mange security awareness and training			X	Manager of Staff Improvement/ Training
Privacy	Coordinate privacy activities in the Agency		X	X	Chief Privacy Officer
Facility	Provide physical security	 X	 X	X	Director of Facilities Facility Managers
Compliance	Ensure regulatory compliance and oversight			X	Compliance Officer
Agency Management	Govern the security management program, evaluate	 X	 X*	X* X* X X	Director of Operations Director of Clinical Programs Director of Human Resources CSO

The Operational Security Team consists of IT and security staff, including those individuals involved in database services, and is jointly lead by the Manager of IT and the Manager of Database Services with oversight by the CSO. The Manager of Charts & Records and her staff are members of this team since they bring functional knowledge around ePHI security.

Staffing for the Rapid Response Team is based on: a) the nature of the incident, and b) the availability of staff resources. The size of the Rapid Response Team depends on the incident and may include Agency business associates or contractors as required.

Members of the QM Team are individuals actively involved in the Agency's decision process for matters related to privacy and security. The Directors of Operations and Clinical Programs jointly lead this interdisciplinary team. There are five voting members, four Agency directors (or designee empowered to make decisions on behalf of that director) and the Compliance Officer. The three advisory members include the CSO, the CPO, and the Manager of Staff Improvement/Training. All voting and standing members are required to attend the Security Management Program Reviews, participate in the on-going security risk assessment process, and take an active role in program evaluation as discussed in Section 7. Other individuals may be invited to participate in QM Team activities if additional knowledge or skills are needed to address a particular issue or situation.

filkins@impulse.net

© 2015 The SANS Institute Author retains full rights.

4.3. Determine Operational Program Requirements

A security program goes beyond just technology. It must start with committed people and resources, both of which are not boundless. In providing an initial budget and timeline, you laid out the work. For now, you have more detailed homework to complete. You now review and formalize these estimates as you establish the program management approach through what will actually be an initial twelve-month project period. The starting point is to close the gaps and remediate the risks identified in the assessment report, but your approach also provides a foundation for ongoing program activities.

You begin with an evaluation of the finding against the elements of your chosen security framework – in this case the HIPAA Security Rule – with a goal to summarize and organize the findings so that program operational requirements, tools, and resources can be identified.

Based on experience you have developed a high-level, standard work breakdown structure (WBS) dictionary "that provides detailed deliverable, activity, and scheduling information about each component in the [WBS]" (PMI, 2013, p.567) which you will use to organize and subsequently tailor to the Agency's program. Table 2 outlines the major elements in this WBS dictionary.

Table 2: WBS Dictionary Elements (Filkins, 2003, p. 18)

WBS Element	Title	Brief Description
1	Security Management Program	Formalized and centralized management structure that creates, administers, and oversees security related policies and procedures to ensure the prevention, detection, containment, and correction of security breaches.
2	Business Continuity and Disaster Recovery	Contingency planning to respond to a system emergency or disaster. Plan is formally documented and periodically tested.
3	Policies and Procedures	An organizational framework that establishes needed levels of information security and privacy to achieve the desired confidentiality goals.
4	Human Resource Procedures	Personnel security and other security related aspects of dealing with employees.
5	Business Associate Agreements	Contract between two business partners for the electronic exchange of data, protecting the integrity and confidentiality of the data exchanged.
6	Security Training and Awareness	Education of the entity workforce regarding security and the reinforcement of that education through on-going reminders to create security awareness as part of the daily responsibilities in the organization.

filkins@impulse.net

© 2015 The SANS Institute Author retains full rights.

WBS Element	Title	Brief Description
7	System / Network Technical Architecture	Standards based architecture that addresses security issues and mitigates risk while meeting entity business and functional needs and requirements.
8	Evaluation	Technical evaluation to establish the extent to which a particular computer system or network design and implementation meet a pre-specified set of security requirements.
9	System and Network Management	Standardized security functions and services applied uniformly throughout the organization, centrally managed with support to the organization's capacity planning, system administration, and network management operations.
10	User Management, Outreach, and Support	Management and support of the end-user environment, incorporating security requirements into the covered entity's IT support structure, an example of which is user interactions with the helpdesk and online knowledge bases.

Each finding from the assessment report is then assigned to one of these 10 elements along with a priority for implementation that is determined as follows:

H = High priority. Associated activities require immediate attention because: a) directly required by Security Rule; b) other actions are dependent on it, or c) actions address an area of high risk or exposure based on a formal risk analysis.

M = Medium priority. Associated activities require timely (i.e., within six months) attention because: a) impediment to full compliance with Security Rule, or b) address an area of medium risk or exposure based on a formal risk analysis. Note: Medium priority activities generally depend on high priority activities. As these high priority activities are completed or resolved, the medium activity may be reclassified as high priority.

L = Low priority. Associated activities require judicious (i.e., within one (1) year) attention because: a) impediment to full compliance with Security Rule, or b) address an area of low risk or exposure based on a formal risk analysis. Note: Low priority activities may depend on medium or high priority activities. These activities may be reclassified as the high or medium activities upon which they depend are completed or resolved.

Finally, based on these assignments, the overall state of Agency compliance with each section of the Security Rule is determined and indicated as follows: ○ = No Compliance; ◗ = Partial Compliance; ● = Full Compliance; and N/A = Not Applicable.

filkins@impulse.net

© 2015 The SANS Institute Author retains full rights.

Table 3 presents the results for the GIAC Behavioral Health Agency, showing the needed emphasis on policy and procedure development, training and awareness, and evaluation tasks, each of which connects to a set of program activities. This type of 'dashboard' allows Agency management to see clearly where to place the initial remediation emphasis as well as how activities involving individual findings might be coordinated. This presentation format can also be used to support the evaluation (Section 7) of on-going program status.

Once assigned to a standard WBS element, each discrete finding can be incorporated logically into Agency-specific plans around privacy and security. By grouping related findings by each WBS element, remediation activities can now be coordinated, effectively scheduled by using a tool like MS Project, and efficiently accomplished with available resources.

filkins@impulse.net

© 2015 The SANS Institute Author retains full rights.

© 2015 The SANS Institute

Table 3: Remediation Findings

Gap Analysis Legend

1 - Security Management Program (WBS 1.0)
2 - Business Continuity & Disaster Recovery (WBS 2.0)
3 - Policies and Procedure (WBS 3.0)
4 - Human Resources Procedures (WBS 4.0)
5 - Business Associate Agreements (WBS 5.0)
6 - Training / Awareness (WBS 6.0)
7 - Technical Architecture (WBS 7.0)
8 - Evaluation (WBS 8.0)
9 - System /Network Management (WBS 9.0)
10 - User Management (WBS 10.0)

WBS Element →		1	2	3	4	5	6	7	8	9	10
Rule/Section	**Gap**										
Administrative Safeguards											
164.308(a)(1)	Security Management Process	◗ H		H	H		H		H		
164.308(a)(2)	Assigned Security Responsibility	◗		L							
164.308(a)(3)	Workforce Security	◗		M	M to H		M				
164.308(a)(4)	Information Access Management	◗		L to H			M	M	H		M
164.308(a)(5)	Security Awareness and Training	◗ H		M			H				
164.308(a)(6)	Security Incident Procedures	◗ H		H					M to H		M
164.308(a)(7)	Contingency Plan	◗	H								
164.308 (a)(8)	Evaluation	◗ H							L to H		
164.308 (b)(1)	Business Associates Contracts	●				M					
Physical Safeguards											
164.310(a)	Facility Access Control	◗ H							M		
164.310(b)	Workstation Use	◗		M						M	
164.310(c)	Workstation Security	◗		M			M	M		L	
164.310(d)	Device and Media Controls	◗ H		M				M			
Technical Safeguards											
164.312(a)	Access Controls	◗		M				L to H			
164.312(b)	Audit Controls	◗		M							
164.312(c)	Integrity	◗						M	M	M	
164.312(d)	Person or Entity Authentication	◗		M				L to M	M		
164.312(e)	Transmission Security	◗						H			
Policies and Procedures and Documentation Requirements											
164.316		◗ H		H							

○ = No Compliance, ◗ = Partial Compliance, ● = Full Compliance, **N/A** = Not Applicable

filkins@impulse.net

Author retains full rights.

4.4. Establish "Book of Evidence" (BOE)

Mark Dill, director of information security at Cleveland Clinic, introduced the concept of a "Book of Evidence" to electronically organize the quantity of information an organization would need to submit to the United States Department of Health and Human Services (HHS) Office for Civil Rights (OCR) if randomly selected for HIPAA audit (Goedert, 2013).

Developing a "book of evidence" (a.k.a. a "book of compliance") for the Agency's program starts with a review of the gap/risk assessment report, advice from industry organizations such as HIMSS (www.himss.org) and WEDI (www.wedi.org), and regulatory guidance from HHS as related to compliance, audit, and enforcement. You will use the Agency's SharePoint site to organize this repository of security artifacts. The BOE should either contain or reference electronic items such as security policies and procedures, program plans, security training and awareness records, and evidence of compliant security controls (e.g., screen shots, log analysis). Suggestions for BOE content are provided in Appendix D.

5. Putting the Strategy Together: Implementation

The next steps is to establish the plan for implementation. Table 4 presents the major objectives, milestones and key deliverables that mark the completion of each milestone, and the suggested progression of how to achieve these milestones over the twelve-month period of performance.

Initializing the security management program is an actual project with its scope defined by the objectives (shown in Table 4), tasks governed by the WBS structure in Table 2, and completion criteria (i.e., transition to recurring program operations).

At this point, your activities will be guided by whatever project management methodology you chose, such as the processes outlined by the five Process Groups defined by PMI (PMI, 2013, p.5). For this effort, you will probably 'borrow' from the artifacts you are developing for the program to guide the initialization project, the charter and the governance plan being among them.

© 2015 The SANS Institute, Author retains full rights.

© 2015 The SANS Institute Author retains full rights.

Table 4: Initial Security Program Implementation Objectives and Milestones

Objective	Key Milestones	Timing (Months from Start)
1. Establish Security Management Program Governance	▪ Select program framework and tools ▪ Develop governance approach and document to include: Program Charter, Governance Plan that defines required governance processes, and metrics to access success ▪ Develop new/update existing plans as identified under governance: risk management, incident response, other ▪ Establish evaluation processes ▪ Establish Book of Evidence repository	1 - 3
2. Establish Risk Assessment and Management Processes	▪ Formalize risk management plan ▪ Develop POA&M ▪ Perform in-depth risk assessment	3 - 4 – perform detailed risk assessment according to finalized risk management plan
3. Restructure Policies and Procedures (P&P)	▪ Develop framework for P&P ▪ Organize committee ▪ Implement framework in SharePoint or ▪ Develop standards for P&Ps ▪ Prioritize P&Ps for development, update and obtain approval	4 - 5 to organize, structure, develop standards Month 5 - 11 to prioritize P&Ps for development and obtain approval
4. Establish Training and Awareness Program	▪ Define training and awareness priorities and requirements, identify existing/free resources ▪ Establish budget ▪ Implement within budget	4 – finalize priorities and requirements, identify resources and budget 4 – 11 implement within budget
5. Evaluate Current Technical Infrastructure	▪ Conduct in-house vulnerability assessment ▪ Align technical vulnerabilities with POA&M	4 - 6 – evaluate and document results 7 – provide recommendations
6. Plan for Security Technology Modernization	▪ Identify improvement/modernization/refresh of technical security controls and conduct cost-benefit analysis around identified areas for modernization ▪ Develop strategic/tactical plan for security technology, coordinate with other Agency and County IT/security tactical (6 to 12 months) and strategic plans (1 – 2 years)	8 - 9 – provide inputs for County/Agency IT plans
7. Conduct Evaluation	▪ Conduct evaluation according to plan, review results, conduct lessons learned	At 6 and 12 months

filkins@impulse.net

© 2015 The SANS Institute Author retains full rights.

6. Making it Happen: Operations

You have your charted course and are now in the air with a flight plan in hand. How should the program appear from an operational vantage point? What are some other elements to consider?

6.1. The Role of the Program Director

Placing a CSO in charge of the security management program will demand a different set of skills than might normally be expected from an individual in that role. Traditionally, a CSO serves as an organization's point of contact for implementation, monitoring, and enforcement of policy, directives and actions, whether mandated by regulations (HIPAA) or by business leaders (Herzig, Walsh, Tuleya, & Healthcare Information and Management Systems Society, 2013, p. 46). He or she is probably familiar with project management.

In the role of program director or manager, however, these responsivities shift and expand, demanding new or improved skills. The program manager is responsible for ensuring that the program continues to meet its overall objectives. He or she needs to coordinate the management of individual projects under the program umbrella, track improvements to the organization's security posture and the reduction of risk, and ensure stakeholders remain committed and actively engaged in organizational security governance. The CSO is now accountable to SC and executive sponsors for schedule, budget, and quality of all program elements.

The CSO will need expanded communication skills, both oral and written, as he will be the conduit between program operations and the SC. These skills include both the delivery of periodic program briefings and status updates as well as the escalation of critical decisions to the executive stakeholders, as required.

Skills related to the facilitation of high-performance teams are valuable. As program manager, the CSO will be expected to lead meetings that will require decision-making by and collaboration among executive-level stakeholders.

The CSO, as program director, will need to review and approve security-related project plans for conformance to program strategy. A CSO may be familiar with project

© 2015 The SANS Institute Author retains full rights.

management, but now he or she will need to understand how to establish milestones and know "when done is done" for concurrent projects under the program's umbrella.

The CSO will need analytics and business intelligence skills to prepare and present meaningful information to stakeholders at various levels. He or she will need to understand how to define and use metrics in discussing the outcomes and quality of the security program as well as to support evaluation and oversight processes (Herzig, Walsh, Tuleya, & Healthcare Information and Management Systems Society, 2013, p. 155).

6.2. The Security Management Process

Figure 2 outlines the operational security management processes you helped define and which the Agency plans to follow. Activities of these teams are coordinated throughout the year with a set of periodic (i.e., annual, quarterly) program reviews led by the QM Team as well as ad hoc meetings convened as a result of a possible incident or actual breach.

The services of each of the teams are shown in this diagram. The exact nature of the service set provided by each team will evolve upon the evaluation of on-going Agency needs, although all activities associated with security governance, such as risk assessment and management, incident response, and change management, should continue to be present.

© 2015 SANS Institute, Author retains full rights.

© 2015 The SANS Institute Author retains full rights.

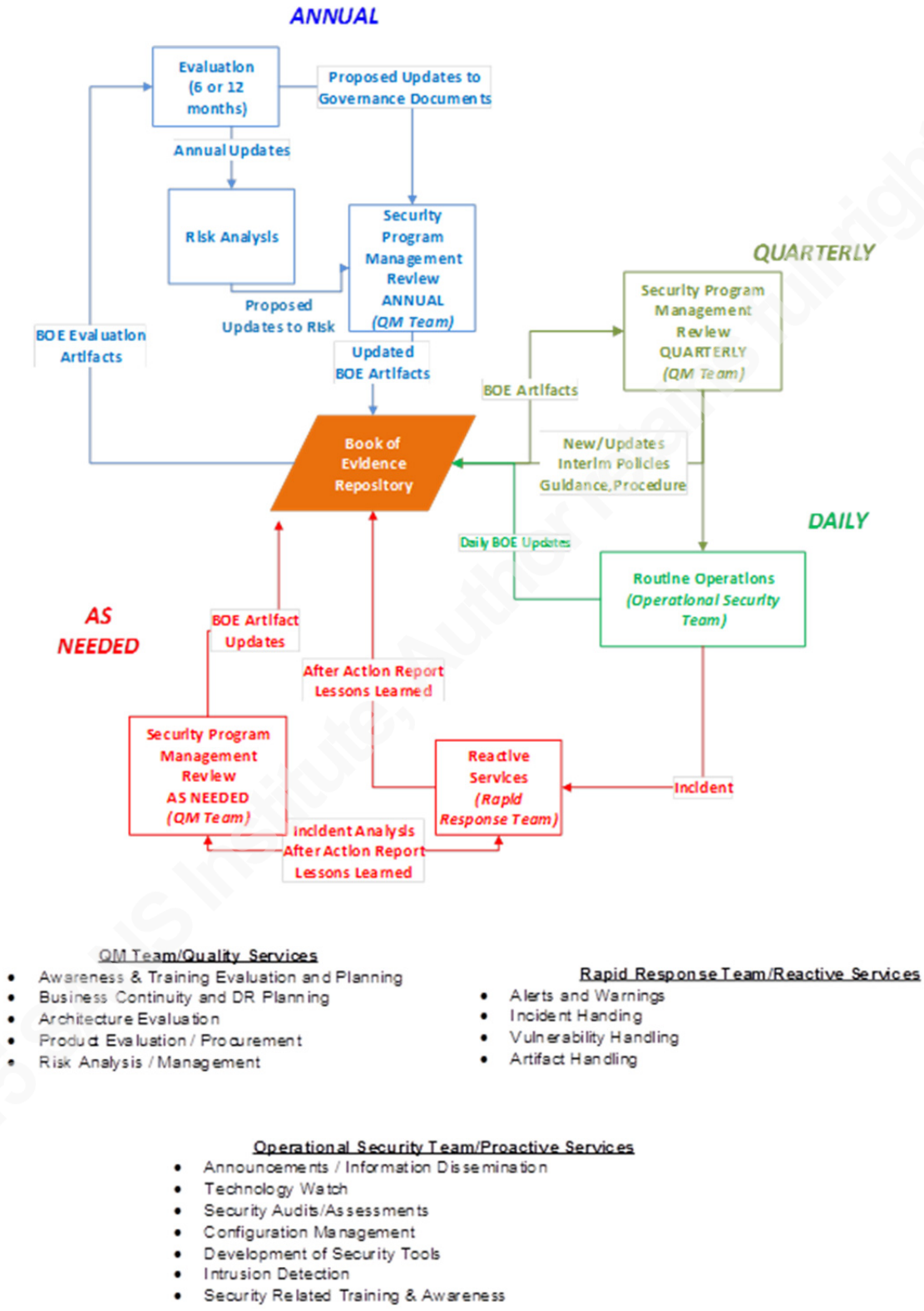

Figure 2. The Security Program Processes and Services

filkins@impulse.net

© 2015 The SANS Institute Author retains full rights.

6.3. Security Management Program Reviews

The process defined in Figure 2 includes periodic program reviews that routinely occur both on a quarterly basis and annually. Quarterly reviews serve as checkpoints throughout the year that the program is achieving its targets for each metric that was defined under governance. The annual review summarizes all security-related activities for that year, including compliance and enforcement events, presents an updated risk baseline and POA&M plan to close the most significant risks, and captures any needed updates to the program charter.

Meeting content normally would include these standard agenda items, not necessarily in order of importance:

- Enforcement review, including any incidents and outcomes, and suggested updates to prevent further incidents or exposure in that area.
- Compliance and performance assessment that covers the following areas: evaluation of existing and new policies and procedures, security training and awareness outcomes, system and network management issues, and upcoming privacy and security concerns.
- Risk management review that addresses updates to the risk inventory and to related POA&M actions.
- Technical review that involves all aspect of the infrastructure, including data, system, and network security. This review could also serve as the security configuration management board.
- Contract and legal review including new business associate agreements or contracts from a security perspective as well as pending procurements.
- Issues and action tracking

7. Evaluating Where You Are

Section §164.308(a)(8)) of the HIPAA Security Rule calls for an organization to "perform a periodic technical and non-technical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or

filkins@impulse.net

© 2015 The SANS Institute Author retains full rights.

operational changes affecting the security of electronic protected health information, which establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart" (HIPAA, 2014).

The operative word here is "evaluation" – if you do not keep track of program performance, you have no idea where you are, what the Agency security posture looks like, where gaps or risks might continue to appear, and what improvements to expect. An evaluation plan, developed under the first objective of Table 4, outlines how the Agency should evaluate its security management program and outcomes to date. Evaluation is not the same as audit, although compliance requirements must be factored into the overall process.

Metrics, discussed previously, are key to determining overall program governance success. Evaluation requires similar attention to the development of appropriate standard procedures and measures used to review systematically an organization's compliance with all the standards and implementation specifications of the HIPAA Security Rule, the selected framework.

There may be overlap with the metrics already established under governance. Evaluation metrics, however, may be more granular. The Agency needs to develop specific performance criteria for evaluation of the extent to which the Agency's controls, starting with its administrative safeguards (i.e., P&Ps), protect ePHI as required by the HIPAA Security Rule in conjunction with applicable HIPAA Privacy Rule requirements.

Evaluation should extend beyond regulatory compliance issues and take into consideration other factors that can influence security such as:

- Effect of security on Agency strategic planning for the acquisition of new technology or upgrades to existing infrastructure. Would it more cost effective to establish a new policy and procedure (a.k.a. administrative control) than invest in a new software capability for access control (a.k.a. technical control)?
- Vendor performance. Are service levels being met and managed?

filkins@impulse.net

© 2015 The SANS Institute Author retains full rights.

- Business associates and contractors. Are the Agency business associates and contractors really secure? Are the appropriate terms and conditions present in partner agreements or contracts to ensure that the Agency can review how business associate and contractors are handling the new emphasis under the HIPAA Omnibus Rule that they must also conform to the same level of security as the Agency?

Of course, evaluation also needs to address the results from the periodic security reviews as to how the program is meetings its key performance objectives.

Next, you need to make the evaluation plan actionable: 1) Document all necessary information that needs to be collected to conduct an evaluation and ensure that this list has been completed in advance of the actual evaluation. (Hint: The BOE should assist here.) 2) Develop and review evaluation procedures, engaging an independent external party if desired to review the approach. 3) Conduct a trial evaluation and document the results, including options exercised, outcomes, recommendations, and remediation decisions. 4) Develop a remediation plan based on the results of the trial evaluation, execute the plan, and provide evidence as to the accomplishments. (Hint: This information should be captured in the BOE.) 5) Evaluate and update the evaluation plan based on as assessment of the trial evaluation process and completeness of its findings.

Evaluation should be conducted both routinely (e.g., annually) as well as when environmental and operational changes occur that could affect the security of ePHI, and when an incident or breach has occurred. According to section §164.306(b)(1) of the Security Rule, the Agency has flexibility in determining its approach to implement the standards and implementation specifications in the Security Rule, but should be prepared to justify its actual approach to evaluation (HIPAA, 2014).

Eventually, the Agency should determine whether internal or external evaluation is most appropriate, depending on resources available, perceived frequency of evaluation, and the need for independent, knowledgeable feedback as to how well the evaluation would meet the requirements of a HIPAA audit. Involvement of the Agency Compliance Officer, CPO, and legal would be good here!

filkins@impulse.net

© 2015 The SANS Institute Author retains full rights.

8. Conclusion

This paper has provided guidance for how to stand up a security management program. Most of the suggestions and examples come from actual, successful implementations.

Remember that security is a cross-functional discipline. Try to structure your security management program so that it involves stakeholders at all levels in the organization. The challenge is to establish committed and effective leadership and management -- processes and people – to avoid an inter-disciplinary approach to security becoming unwieldy.

The key to success is to understand (and demonstrate) what is meant by governance as it applies to the organization and then how that ties into security governance within the organization. Organizational governance has become an extremely popular concept today but the term lacks an exact definition. It depends on the organization's overarching mission statement as well as and what the organization needs to accomplish. Likewise, the definition of security governance is broad and varies widely in implementation. Do not neglect the program charter, governance plan, and well-defined metrics that show how the program is achieving actual targets that support its critical success factors. These artifacts may become the program's lifeline to existence.

Consider the all-important human element, especially in the process and data-intensive environment that is healthcare. True success requires that the program instill security awareness, acceptance, compliance, and competence across workforce members. Consider how to meet the following objectives throughout the entire security management program, not just specific to security training and awareness component:

- Engage the workforce (staff, contractors, and where appropriate consumers or patients) as participants in privacy and security through an outreach campaign that informs and promotes community awareness about related issues and the benefits of the security management program.
- Maintain this engagement through formal and informal education that is informative in content and practical in nature, backed by a strategy to increase

filkins@impulse.net

© 2015 The SANS Institute Author retains full rights.

community understanding as well as awareness around related issues and program benefits.

- Incorporate training on privacy and security best practices into the organization's overall training program for the use, operation, and administration of its information assets. The best approach is to use scenario-based training and performance-based appraisal – does the user understand the reason for action and select the proper approach?

Match program roles with the organizational structure and, most importantly, select the program director or manager with care. The skill set for this individual goes beyond what may be expected of the standard CSO. He or she will need to know how to manage at a broader scope than a specific project. He or she will need strong communication skills, both written and verbal, but just as importantly will need to be able to facilitate the cross-functional teams needed for program success.

QM and evaluation are key. Both can keep the organization out of trouble and, done correctly, can provide needed short-term oversight and direction by continually reviewing performance against the specific measures required for robust security and compliance.

The bottom line is that effective security will involve organizational culture change. The challenges are keeping things simple for the end-user, using common sense, and avoiding complicated processes that do not match the business needs of the organization. It does not matter if better security demands a new process – processes impedes the business workflow, like providing patient care, will not be used. In fact, the organization may end up less secure than before!

filkins@impulse.net

© 2015 The SANS Institute Author retains full rights.

References

Allen, J. (2005). Governing for Enterprise Security (Technical Note CMU/SEI-2005-TN-023). Retrieved from Software Engineering Institute, Carnegie-Mellon University website: http://www.sei.cmu.edu/reports/05tn023.pdf.

Filkins, B. (2014, December). New Threats Drive Improved Practices: State of Cybersecurity in Health Care Organizations. Retrieved January 14, 2015, from https://www.sans.org/reading-room/whitepapers/analyst/threats-drive-improved-practices-state-cybersecurity-health-care-organizations-35652.

Filkins, B. (2003, July). Getting Started: The Impacts of Privacy and Security Under HIPAA. Retrieved January 17, 2015, from http://www.sans.org/reading-room/whitepapers/hipaa/started-impacts-privacy-security-hipaa-case-study-1214

Goedert,J. (2013, May 1). Ready or Not, Here Come HIPAA Audits - Health Data Management Magazine Article | Health Data Management. Retrieved January 15, 2015, from http://www.healthdatamanagement.com/issues/21_5/hipaa-privacy-security-breach-enforcement-audit-ocr-46079-1.html?pg=3

Granneman, J. (2013, September). IT security frameworks and standards: Choosing the right one. Retrieved from http://searchsecurity.techtarget.com/tip/IT-security-frameworks-and-standards-Choosing-the-right-one

Health Insurance Portability and Accountability Act of 1996 (HIPAA), 45 C.F.R § 164 (2014).

Health Insurance Reform: Security Standards; Final Rule, 68 Fed. Reg. 8334 (February, 20, 2003) (to be codified at 45 C.F.R. pt. 160, 162, & 164).

Herzig, T. W., & Healthcare Information and Management Systems Society. (2010). *Information security in healthcare: Managing risk.* Chicago, IL: HIMSS.

Herzig, T. W., Walsh, T., Tuleya, L. G., & Healthcare Information and Management Systems Society. (2013). Implementing information security in healthcare: Building a security program. Chicago, IL: HIMSS.

Mont, J. (2014, September 23). Compliance Deadline for New HIPAA Privacy Rules Arrives | Compliance Week. Retrieved January 14, 2015, from http://www.complianceweek.com/blogs/the-filing-cabinet/compliance-deadline-for-new-hipaa-privacy-rules-arrives#.

filkins@impulse.net

© 2015 The SANS Institute Author retains full rights.

Pritts, J. (2003, April). Preemption Analysis Under HIPAA: Proceed with Caution. Retrieved January 16, 2015, from http://library.ahima.org/xpedio/groups/public/documents/ahima/bok3_005197.hcsp?dDocName=bok3_005197

Project Management Institute. (2013). *A guide to the Project Management Body of Knowledge (PMBOK guide), fifth edition.* Newtown Square, Pa: Project Management Institute.

Summary of the HIPAA Security Rule. (n.d.). Retrieved January 14, 2015, from http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html.

West-Brown, M., Stikvoort, D., Kossakowski, K. -P., & CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST. (2003). Handbook for Computer Security Incident Response Teams (CSIRTs) (2nd ed.). Retrieved from http://www.sei.cmu.edu/reports/03hb002.pdf.

filkins@impulse.net

© 2015 The SANS Institute Author retains full rights.

Appendix A: Glossary

Acronym	Definition
BOE	Book of Evidence
BYOD	Bring Your Own Device
C.F.R.	Code of Federal Regulations
COBIT	Control Objectives for Information and Related Technology
CPO	Chief Privacy Officer
CSO	Chief Security Officer
EHR	Electronic Health Record
e-PHI	electronic protected health information
FISMA	Federal Information Security Management Act of 2002
GIAC	Global Information Assurance Certification
HHS	Health and Human Services
HIMSS	Healthcare Information and Management Systems Society
HIPAA	Health Insurance Portability and Accountability Act of 1996
ISO	International Organization for Standardization
IT	Information Technology
NIST	National Institute of Standards and Technology
OCR	Office of Civil Rights
ONC	Office of the National Coordinator
P&P	Policies and Procedures
PII	Personally Identifiable Information
PMBOK	Project Management Body of Knowledge
PMI	Project Management Institute
PMT	Program Management Team
POA&M	Plan of Action and Milestones
QM	Quality Management
SC	Steering Committee
WBS	Work breakdown Structure
WEDI	Workgroup for Electronic Data Interchange

filkins@impulse.net

© 2015 The SANS Institute Author retains full rights.

Appendix B: Program Charter Table of Contents

#	Section	Contents
	PREAMBLE	This includes: • Cover Page • Charter Approval Block • Document Revision History • Table of Contents • List of Figures and Tables
1	INTRODUCTION	Succinctly state purpose of the document. Example: The Agency Security Program Charter establishes the Program vision, objectives, scope, and governance structure, including the participant and stakeholders roles, responsibilities and relationships for this partnership. State when the document will be reviewed and updated. **Example:** The Security Program Charter will be reviewed and updated as needed on an annual basis.
2	BACKGROUND	**(Optional)** Provide any needed background for the reader to understand the elements in the Program Charter. This can include the current problem statement and history behind the Security Program.
3	PROGRAM CONCEPT	Provides elements that define the Program concept.
3.1	PROGRAM GOAL STATEMENT	State what the overall goal of the Program is. This can be considered the mission statement. The goal should be reviewed and updated on an annual basis. **Example:** The goal of the Security Program is to protect the Agency through reducing the risk and creating an internal culture of privacy and security while enabling it to meet its mission of providing the highest quality care to its clients.
3.2	PERFORMANCE OBJECTIVES TO ACHIEVE PROGRAM GOAL	Document a set of progressive objectives that will allow the Agency to achieve its stated goal. A set of objectives should be defined for each year, preferably three but no more than five. Performance objectives should be consistent with the Agency strategic plans, especially IT, and should be stated so that metrics can be established to gauge success and progress. These objectives should be reviewed and updated on an annual basis, whether or not the Program goal changes. **Example of performance objectives by year:** Year One: • Establish Program governance structure • Establish Book of Evidence (security repository) in SharePoint • Achieve 10% reduction in current risk posture • Hold five security awareness events • Evaluate automated tools for vulnerability testing • Conduct Program evaluation Year Two:

filkins@impulse.net

© 2015 The SANS Institute Author retains full rights.

#	Section	Contents
		• Procure policy management system • Hold ten security awareness events • Procure automated tools for vulnerability testing • Achieve 20% reduction in current risk posture • Conduct Program evaluation
3.3	PROJECT SCOPE	Define what is in and out of the Program scope. **Example:** The Program scope includes: • Participation in Agency change management processes representing privacy and security concerns • Development of system-specific security policies and procedures related to Agency information system assets The Program scope does not include: • Participation in County change management processes
3.4	SOLUTION VISION	**(Optional)** Develop a key statement with Agency stakeholders that can be used to focus the Program on actual privacy and security needs and desired improvements it can provide for the Agency.
3.5	CRITICAL SUCCESS FACTORS	Document those generic Program activities and items that, if adequately addressed at the appropriate time will increase the probability of the Program being successful. **Example:** Critical success factors related to governance are: • Continuing support for the Program from Agency executive leadership • Single point of leadership empowered to lead the Program • Multi-disciplinary Program teams empowered to execute defined security services
3.6	PROGRAM ACTIVITIES	High-level overview of program activities and, where applicable, work products associated with each. See Figure 2.
3.7	ASSMPTIONS AND CONSTRAINTS	**(Optional)** State known assumptions and constraints. These assumptions and constraints will be analyzed, validated periodically, and updated if needed as the Program matures. **Example:** Assumption: The Program risk and change management processes for security will align with and be managed as part of the Agency-wide processes in this area. Constraint: Administrative policies and procedures will have to be implemented around access management until Agency budget permits purchase of the appropriate technology.
3.10	PRROGRAM IMPACTS	**(Optional)** Define how the Program may impact the Agency and how it conducts business.
3.11	SUCCESSFUL COMPLETION CRITERIA	Criteria for determining Program success as mapped to Program goals, objectives, and established controls. These may not be the exact metrics, but should be unambiguous, observable and traceable back to Program goals and the progressive objectives for success. These criteria should also be traceable to governance metrics. Criteria will be reviewed

filkins@impulse.net

© 2015 The SANS Institute Author retains full rights.

#	Section	Contents
		and updated on a yearly basis.
4	ORGANIZATION	Document high-level governance structure. Further discussion will be provided in the Governance Plan. Include: roles and responsibilities for positions and organizations supporting the Program; Program stakeholders that may or may not have direct responsibility for Program activities but whose participation and support is essential to Program success

© 2015 SANS Institute, Author retains full rights.

filkins@impulse.net

© 2015 The SANS Institute Author retains full rights.

Appendix C: Governance Plan Table of Contents

#	Section	Contents
	PREAMBLE	This includes: • Cover Page • Charter Approval Block • Document Revision History • Table of Contents • List of Figures and Tables
1	INTRODUCTION	Defines the purpose of the document.
1.1	PURPOSE	Succinctly state the purpose of this document. **Example:** "The purpose of a formal governance structure is to steer, control and manage the Program. The purpose of the Program Governance Plan is to document the governance structure for the program and the purpose of governance.
1.2	SCOPE	Define the scope of the document, what it covers. **Example:** "This document describes the three (3) main governance bodies for the Security Program (the Steering Committee, the Program Management Teams, and the Integrated Project Teams), their roles and responsibilities, and the structure of each."
1.3	REFERENCES	List the sources referenced in this plan, including external plans that may apply.
1.4	DOCUMENT MAINTENANCE	Document when the document is reviewed and updated. **Example:** "This document will be reviewed annually and updated as needed."
2	GOVERNANCE ROLES AND RESPONSIBILITIES	This section outlines the structure for Program Governance.
2.1	AGENCY ORGANIZATIONAL STRUCTURE	Describe the organization structure of the Agency and how it maps into the Program structure.
2.2	PROGRAM STRUCTURE	Describe how the Program structure is organized. See Figure 1.
2.3	ROLES AND RESPONSIBILITIES	Detail the roles and responsibilities of key governance positions.
3	STEERING COMMITTEE	Describe the purpose, scope, membership and procedures for the Program Steering Committee.
3.1	PURPOSE	**Example:** "The Program Steering Committee is a decision-making body -body for privacy and security matters that affect the Agency. The SC also fosters collaboration across Agency organizational boundaries, bringing enterprise needs and policy perspective to the Program."
3.2	SCOPE	**Example:** "The SC is not directly responsible for managing project activities, but provides support and guidance for those who do."
3.3	MEMBERSHIP	This provides the list of members and their roles on the SC.
3.4	PROCEDURES	This section outlines the procedures followed by the

filkins@impulse.net

© 2015 The SANS Institute Author retains full rights.

#	Section	Contents
		SC to include communications, meetings schedule, conduct, and voting protocols.
4	PROGRAM MANAGEMENT TEAM	Describe the purpose, scope, membership and procedures for the Program Management Team
4.1	PURPOSE	**Example:** The Program Management Team (PMT) is responsible for ensuring Program outcomes are achieved as outlined in Program Charter and last evaluation report.
4.2	SCOPE	Scope here means those governance activities that directly affect the sustainability of the Program. See Table 5 below.
4.3	MEMBERSHIP	Describe the three teams and the membership of each.
4.4	PROCEDURES	Refer to applicable plans and procedures for the operation of the Program, such as management reporting, incident response, and so forth.
5	INTEGRATED PROJECT TEAMS	**(Optional)** Situations involving privacy and security will arise that will require specific projects. This section outlines how Integrated Project Teams (IPTs) can be used to formally address the specific situations that require a cross-functional team to develop and execute strategies and plans to resolve the issue. **Example:** An Agency management review indicates a previously unrealized threat that will require coordination between several County entities to mitigate its risk. The scope of this effort is beyond the normal capabilities of the Program Management Team. It will require the involvement and commitment of the larger community to develop a strategy plan and execute the strategy through a Program-led project.

Governance will be sustained by a set of activities, for either which the security program is responsible or in which it will play a key (i.e., stakeholder) role. Table 5 defines each governance procedure, indicates the main reference that outlines how each will be implemented in this program, and the primary authority associated with the activity.

Table 5: Security Management Program Governance Activities

Governance Activity	Elements	
Project Management	Define:	Manage individual security-related projects on a daily basis across all stages from project initiation through development to the transition to operations.
	Reference:	Master Project Plan and associated plans
	Authority:	Program Manager, Specific Project Management
Issue Management	Define:	Identify, manage, resolve issues that arise during the program
	Reference:	Security Issue Management Plan
	Authority:	Issue Manager, Issue Management Team
Risk Management	Define:	Identify, manage, mitigate risks identified during the program

filkins@impulse.net

© 2015 The SANS Institute Author retains full rights.

Governance Activity	Elements	
	Reference: Authority:	Risk Management Plan Risk Manager, Agency Risk Committee
Quality and Performance Management	Define: Reference: Authority:	Establish standards, metrics, and indicators for program quality and performance, monitor project progress, and manage corrective actions to maintain established standards. Quality Management Plan, Performance Management Plan Quality Manager, Program Manager
Change/Configuration Management	Define: Reference: Authority:	Manage the process of controlling and implementing major changes within Agency that either will affect information security or be affected by security in terms of business process, automation, and supporting technology to reduce the risk and cost of change, and to optimize its benefits. Establish and maintain consistency of the Agency baselines throughout the project and system life cycles. Change Control and Configuration Management Plan Change Management Team, Agency Change Control Board (CCB)

filkins@impulse.net

© 2015 The SANS Institute Author retains full rights.

Appendix D: Suggested Contents for Book of Evidence

A "book of evidence" is a repository or library of security artifacts. A suggested list of contents includes:

- Policies, plans, and procedures, referenced appropriately as to location either physical or electronic.
- Key plans that outline Agency security activities such as risk management, training and awareness, contingency, and incident response. These plans can be created independently as part of Agency security management program or can be incorporated into existing Agency plans, but should be recognizable as security program artifacts.
- Change management/versioning records related to a) policies and procedures, b) information system changes, and c) other critical items that affect the privacy and security of ePHI.
- Evidence of accomplishments including meeting agendas and minutes, completed reviews of information system activities like audit and access logs, delivery of security training and awareness, security incident reports along with lessons learned, and validation testing for business continuity/disaster recovery process and outcomes.
- Security training and awareness manuals and materials.
- Asset/system inventory, covering both authorized and unauthorized devices and software.
- System security plan for key information systems that manage ePHI (EHR, practice management system) that delineates system-specific controls and configuration.
- Inventory of screen shots, reports, and other items that demonstrate compliance.
- Periodic evaluation procedures, outcomes, and Plan of Action and Milestones (POA&M) for remediation of finding.

filkins@impulse.net

© 2015 The SANS Institute Author retains full rights.