

# Why Security and Risk Analysis are a must for HIPAA Compliance and Meaningful Use Attestation?

## Security Analysis

The task of managing security is complex. Over 32K security gaps are now documented as potential vulnerabilities and are growing alarmingly. The recently discovered vulnerabilities that were lying dormant for years, such as the Heartbleed, shell shock, and poodle bugs, and the recent GHOST vulnerability have added new dimensions to the security gaps.



Many of the new path breaking technology developments, may not have factored the safety and security components adequately during their development, introduction in the market and their very fast acceptance due to their appeal. The interconnectivity of these new devices is leading us to voluminous data availability and exposure via, smartphones, Internet of Things (IoT), cloud-based - applications, authentication and storage solutions. Pieces of information picked up from these huge number of connected devices, and big data analytics could open new sources of information exploitation by the organized cyber criminals from volumes of information.

Over 92K checks must be performed to assess the status of security of your infrastructure across your physical and virtual networks, operating systems, databases, and Web applications.

With sophisticated tools, cyber-attackers unfortunately, have asymmetric advantages over businesses.

**The need for security analyses stems from the regulatory requirement (45 C.F.R. §§ 164.302 – 318.) This is to help entities in identifying and implementing the most effective and appropriate administrative, physical, and technical safeguards to secure electronic protected health information (e-PHI).**

All e-PHI created, received, maintained or transmitted by an organization is subject to the Security Rule. The Security Rule requires entities to evaluate risks and vulnerabilities in their environments and to implement reasonable and appropriate security measures to protect against reasonably anticipated threats or hazards to the security or integrity of e-PHI. Risk analysis is the first step in this process.

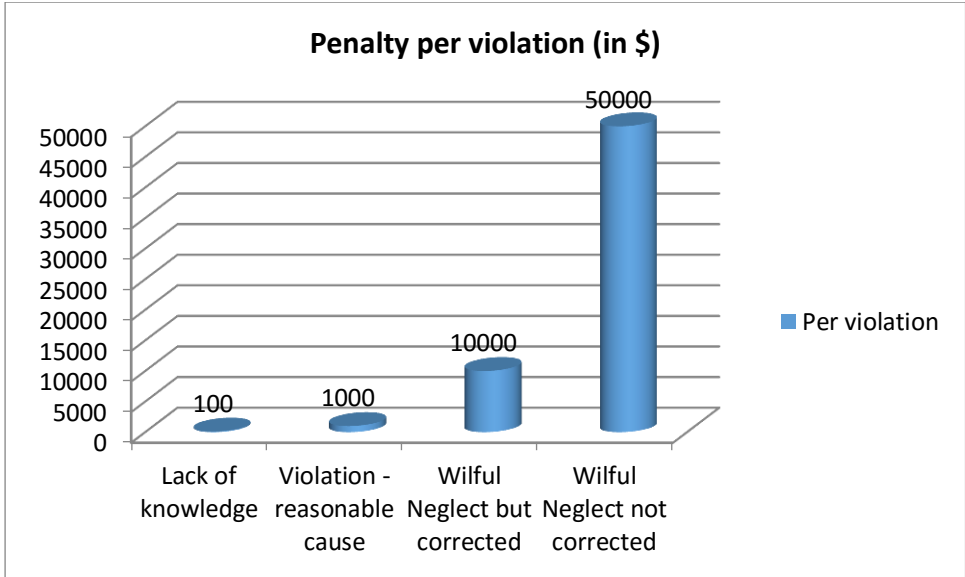
The penalties are severe; the second reason why organizations must do a security analysis. For instance, the end of 2014 saw Anchorage Community Mental Services (ACMHS) settlement for potential violations by paying \$150,000 and adopt a corrective action plan to correct the deficiencies in its HIPAA Compliance Program.

### HIPAA Penalties (\$)



	<b>Per violation</b>	<b>Annual Max for repeat violation</b>	<b>Max penalty per violation</b>	<b>Annual max penalty</b>
Lack of knowledge	100	25000	50000	1500000
Violation - reasonable cause	1000	100000	50000	1500000
Wilful Neglect but corrected	10000	35000	50000	1500000

Wilful Neglect not corrected      50000    1500000      50000    1500000



If Security analyses and risk management are not effectively implemented, the violation will be categorized as ‘Wilful Neglect not corrected’.

You must be conscious of the security challenges that you need to address in the first place.

### The Security Challenges

- Knowing when assets that affect business in real-time are added/removed by people.
- Determining how to implement complex security tools and where to acquire the required technical skills.
- Managing a large number of vulnerabilities continuously.
- Managing isolated, silo solutions against 35,000+ security controls to remain compliant under various mandatory business regulations and standards.
- Determining a risks-management methodology that is appropriate.

Managing security does not end with these challenges—many more how-to questions need to be addressed.

**Aegify SPM helps you assess your security posture accurately identifying security gaps, prioritizing and fixing (remediation) them in a timely manner and avoid stiff penalties and adverse publicity.**

## Risk Analysis

After doing security analyses the next important step is to do a risk assessment. After the security gaps are identified the risk analysis helps to study the impact of unknown threats likely to occur now or in the future, exposing to a chance of loss or damage. **Security Risk plus Compliance Risk is a very big Business Risk.**

### Risk Analysis Requirements under the Security Rule

The Security Management Process standard in the Security Rule requires organizations to “[i]mplement policies and procedures to prevent, detect, contain and correct security violations.” (45 C.F.R. § 164.308(a)(1).) Risk analysis is one of four required implementation specifications that

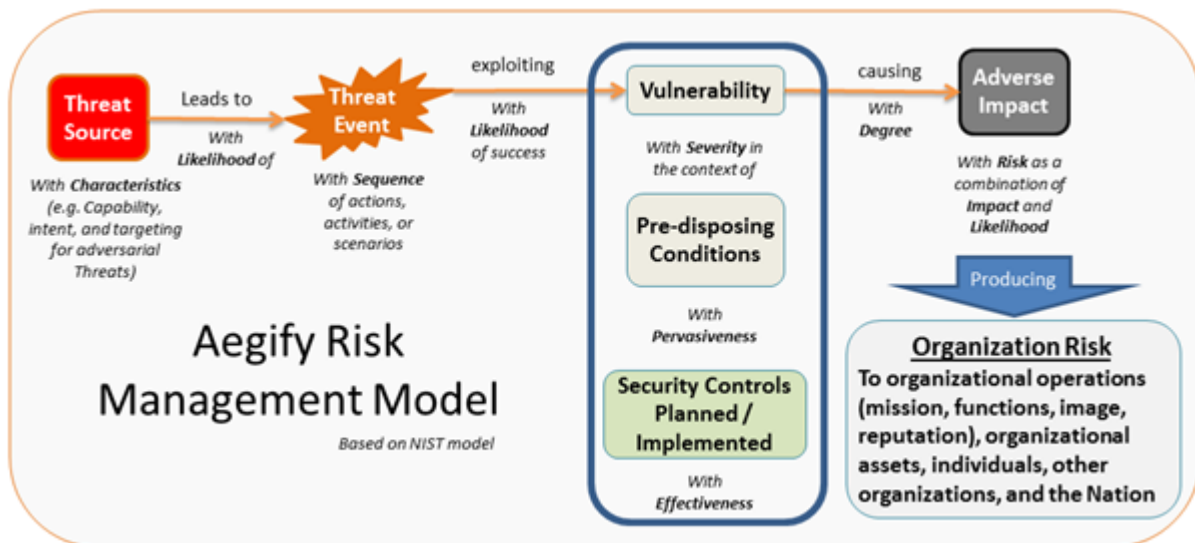
provide instructions to implement the Security Management Process standard. Section 164.308(a)(1)(ii)(A) states:

“RISK ANALYSIS (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the [organization].”

The information security context must be understood as illustrated below:



Aegify Risk Management Model helps you minimize your risks



### About Aegify Risk Manager

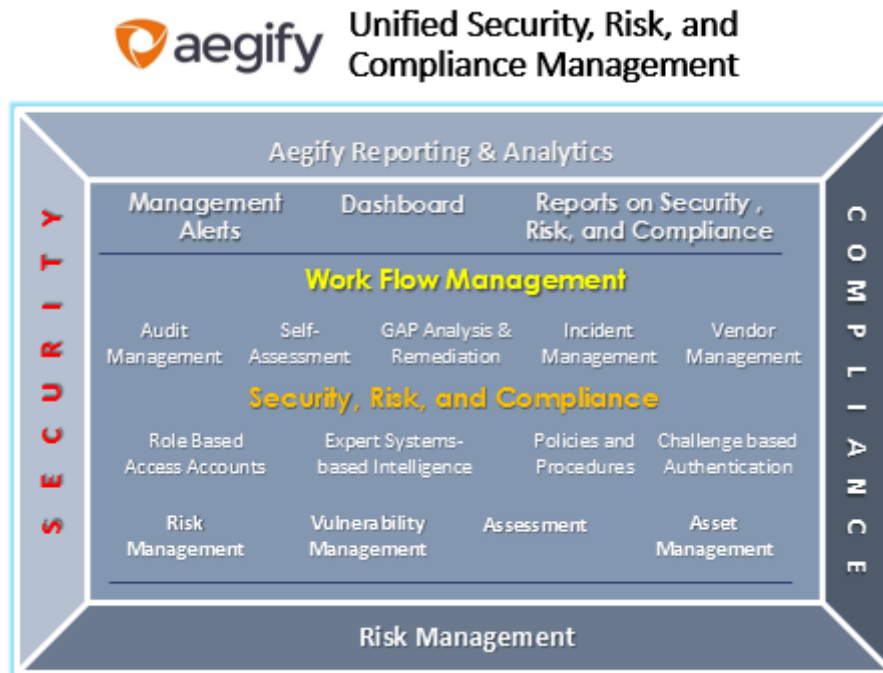
- Features the world’s first cloud-based service that provides real-time continuous monitoring of risk, security, and compliance status.
- Helps you automate risk management using built-in expert system leveraging best-practice inputs from standards such as NIST, ISO, and OCTAVE among others.
- Helps you define the asset-based risk factors and the relationships among those factors - threat, vulnerability, impact, likelihood, and predisposing








- By significantly reducing the time to demonstrate meaningful use that otherwise takes about 70% time
- By safeguarding electronically stored data with its advanced monitoring capabilities
- By providing instant built-in support for all HIPAA/HITECH regulations
- By its ability to collect and store all HIPAA-related provisions and related documents online into a single repository, making it a hands-on tool and thereby easier to use and access.

## Aegify – Security, Risk, and Compliance Integrated Solution



### Six Easy steps with Aegify for dealing with Security, Risk and Compliance Management

1. **Auto-discover security, risk and compliance issues** - Some assets are critical to your business. Tracking such assets from threat and vulnerability perspectives and estimating the risks effectively, provides you with a quick blueprint for action to mitigate risks from operating systems, network devices, firewalls, Intrusion detection systems, web applications, databases, adware or spyware, etc. Aegify does a complete scan and populates the compliance controls with automated answers and makes it easier for assessment, audit review, and implementing remedial measures, speeding the audit process with its auto-review and cross-system impact analysis features. 
2. **Cloud-Based Security Posture and Self-Assessment using an Expert System** - Simplifies the compliance assessment survey for users on topics such as privacy, security, and procedures related to a regulation or standard requiring compliance. During the survey, users have access to extensive online help that makes answering questions easy. As the survey is completed, the software analyses responses and gathers strong as well as weak practice segments. An Expert system will automatically map the Security scan results to Compliance Control Organizations then receive a complete snapshot of their compliance and risk status that can be viewed online at any time. 
3. **Upload Compliance Documents Into a Policy Management Portal** - As organizations complete the assessment, attaching documentary evidence of 

policies, procedures, practices or agreements with business associates, is simple. Users will be prompted to upload them to Aegify document repository that is required as part of the audit review.

4. **Assess your risks** - Aegify helps you assess your risk through a systematic algorithmic analysis fine tuned to the regulatory requirements. Aegify will generate a GAP report with prioritized recommendations for every missing Security, Risk and Compliance issue that is identified.



5. **Remediation and Action Roadmap** - Aegify helps you assess your risk through a systematic algorithmic analysis fine tuned to the regulatory requirements. Aegify will generate a GAP report with prioritized recommendations for every missing Security, Risk and Compliance issue that is identified.



6. **Complete Remediation and Continuous Monitoring** - Organizations can address the "To-Do" items at their own pace while remembering that completing the compliance report may have deadlines dictated by the regulation. Multiple Assessment and Remediation Cycles can be scheduled to ensure continuous monitoring.



A Step-by-Step Approach for your enterprise to Comply with the latest HIPAA ... At your own Pace... with help from Aegify.

