

White Paper

Security, Risk and Compliance (SRC) – Tech-enabled Functional Perspective



Table of Contents

Secure, multi-tenanted, framework-based Architecture	3
Unique Security features.....	3
AWS Infrastructure.....	3
Instance Isolation:	3
Aegify Application Security	4
Multi-tenanted architecture:	4
Customer data protection.....	5
Multi-dimensional Data Analysis.....	5
7-D Data Normalization	6
Governance Parameters.....	6
Aegify GRC Framework	7
Compliance Framework:	7
Unified and Integrated Security, Risk, and Compliance Management	8
Key components of Aegify	8
Security Posture Management (SPM)	8
Perimeter Scanning	10
Aegify Compliance Manager	11
Vendor Management	13
Aegify Risk Manager	14
Meaningful Use Grants	15
Automated SRC Processes.....	16
Automation of SRC Governance process makes a big difference –	16
Aegify automation features	17
Extensive Reports and dashboard views for quick remedial action and and audit preparedness with What-if-Analysis	17
Assessment reports	18
Asset Management Reports	18
Risk Reports.....	18
What-if-Analysis	18
Security Posture and Risk Heat Map Reports	18
Exclusive Partner Portal	19
Distinct features of Aegify Summarized	19

Secure, multi-tenanted, framework-based Architecture

Aegify was architected and engineered with complete cloud focus and first of integrated security, risk, and compliance services that is SaaS based. Aegify was built on a cloud architecture that is event driven, recovery and service oriented architecture and based on seven Dimensional Multi Stage Data Normalization.

Unique Security features

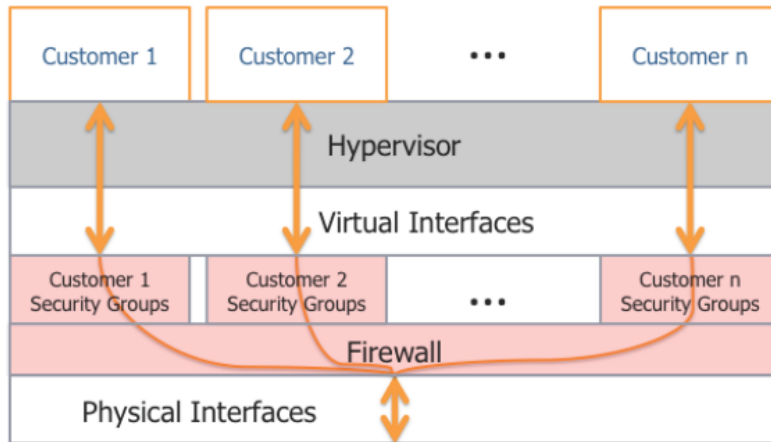
AWS Infrastructure

Aegify is hosted on Amazon Web Services (AWS) Cloud Infrastructure

- AWS is compliant with various certifications and third-party attestations such as SAS70 Type II, PCI DSS Level 1, ISO 27001, and FISMA.
- The Flexibility and customer control that the AWS platform provides permits the deployment of solutions that meet industry-specific certification requirements such as healthcare applications to measure compliance levels with HIPAA / HITECH Security and Privacy Rules or the Payment Card Industry Data Security Standards (PCI-DSS), or a wide range of compliance regulations and standards such as FISMA, COBIT, ISO 27K, etc., on AWS.
- With Amazon's many years of experience in designing, constructing, and operating large-scale data centres throughout the world, its infrastructure and the location is accessible within Amazon only to those who have a legitimate business need to have such. A variety of physical barriers in these data centres add to ensuring only authorized access.
- AWS enables users to encrypt their personal or business data within the AWS cloud and publishes backup and redundancy procedures for services.
- Amazon Web Services has successfully completed multiple SAS70 Type II audits. SAS70 certifies that a service organization has had an in-depth audit of its controls.
- Security exception monitoring mechanisms provide adequate protection for Aegify against Distributed Denial of Service (DDOS) attacks, Man-in-the-middle (MITM) attacks, IP Spoofing, unauthorized Port Scanning, packet sniffing, etc.
- Each of the services within the AWS cloud is architected to be secure and contains a number of capabilities that restrict unauthorized access or usage. AWS provides a highly scalable, reliable, and inexpensive data storage infrastructure that offers dependable backup solutions.

Instance Isolation:

AWS Architecture enables their customers to use a single code base with dynamic virtual partitioning of the system. The information is virtually partitioned in the cloud. Virtual partitioning helps to isolate the data for each customer and easy data manageability.



To ensure privacy and security of data of each client that uses our cloud services, different instances running on the same physical machine are isolated from each other via the Xen hypervisor. In addition, the AWS firewall resides within the hypervisor layer, between the physical network interface and the instance's virtual interface. All packets must pass through this layer, thus an instance's neighbours have no more access to that instance than any other host on the Internet and can be treated as if they are on separate physical hosts. The physical RAM is separated using similar mechanisms.

Customer instances have no access to raw disk devices, but instead are presented with virtualized disks. The AWS proprietary disk virtualization layer automatically resets every block of storage used by the customer, ensuring that one customer's data are never unintentionally exposed to another.

Aegify Application Security

Access Control:

The innovative and granular Access Controls (Label Based and Role Based Access Controls) give the control to the end user to protect their data.

- LBAC model applies labels (Access Domain and Access Level) to users to define which account/customer the user can access.
- RBAC model applies roles to users so that access to any feature/data in the system will be based on the Role defined in the system.

All interactions and user/client identification is through SSL/HTTPS. The password policy enforced is as per de facto industry usage with password expiry, strength and validation aspects built in.

Multi-tenanted architecture:

Multi-Tenant Architecture of Aegify enables the customers and partners to use a single code base with dynamic virtual partitioning of the system. The information is virtually partitioned in the cloud. Virtual partitioning helps to isolate the data for each customer and easy data manageability.

Aegify Customers' data is in a database and spread across multiple tables. Database access is restricted to the Database Administrator. Virtual partitioning is done by using Role-based and Label-based access control.

Aegify also provides customer specific customization such as embedding the partner logo that will display to all the partner's customers.

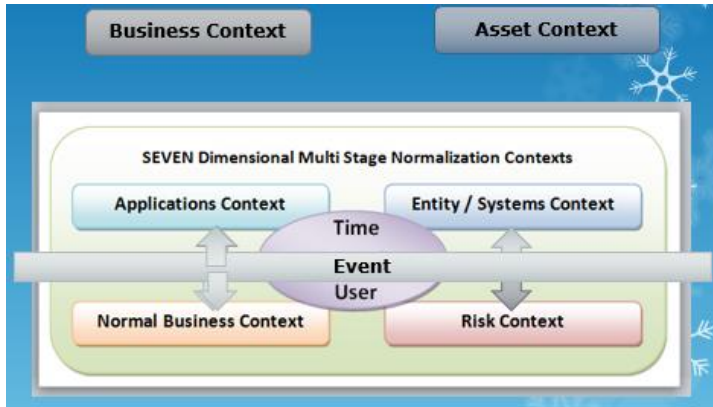
Customer data protection

Aegify cloud services covers information relating to accounts and processes, regulatory controls or standards mapped to different clients, password policy, user management accounts, role-based module access rights, assessment templates and the associated response data and documentary attachments, reviewed data from auditors, assessment data such as gaps identified, corrective steps undertaken, etc.

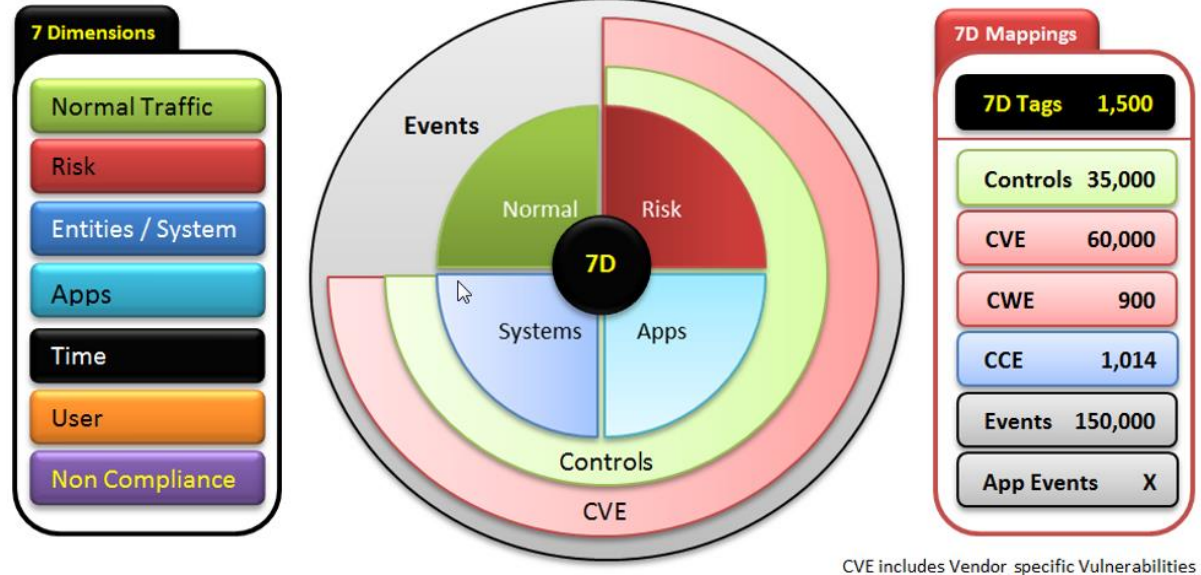
- A Keystore is installed on Aegify to encrypt files. Keystore is a database of keys in which, Private keys have a certificate chain associated with them, which authenticates the corresponding public key. A keystore also contains certificates from trusted entities. Different Keystore has been implemented in different environments such as Quality Assurance, Development, and Production. The Keystore file being password protected and changed every few months programmatically that ensures absolute security of the data.
- The data while being sent from the customer premises to the cloud is encrypted using 3-DES symmetric encryption. Types of files that are encrypted include- evidence files, security scan outputs. Security scan configuration XML, Policy files not supplied out of the box by Aegify, customer or partner uploaded documents. With client and server side authentication, the data in transit will be secure.
- Aegify tokenizes all individually identifiable data of customers. The tokenization information is segregated from the actual data so as to make it practically impossible for anyone trying to make sense of the data outside of the programmatically implemented access control mechanism of Aegify.
- Aegify Customer data in the cloud is secured using the state-of-art encryption mechanisms. Vulnerability Scan data and all other security related data in the file system are encrypted as part of secure storage.
- Aegify Customer may use a separate customer specific key to encrypt all their data for which a new Keystore is generated for 3-DES symmetric encryption. Customer Keystore is password protected and is not stored in Aegify. {This is a feature under development and will be available in a future release}.
- On the cloud, the data will not be accessible to either the Aegify employees or the Cloud-Service provider personnel. Only Production operations Admin or the Database Admin will have access to the Aegify Server or Database and no one else will access to customer data. Each customer's data will be completely isolated from any other customers. The cloud provider's strong security measures as explained under other questions, provides a strong and secure framework.
- Secured continuous replication of the data ensures the data persistence.

Multi-dimensional Data Analysis

Aegify's context specific and multi-dimensional Data analyses helps in prioritizing the risks and critical controls by which protection measures implemented could be most effective. In addition the harmonized controls helps organizations quickly map to different regulations and standards in one shot simplifying the rigor of assessing under different compliance requirements through automated mapping of related controls.



7-D Data Normalization



Multi-dimensional data analysis and 7-D normalization helps in correlating, application/entity/system events with context specific Risk and Compliance controls. The 7-D normalization also helps in correlating application and system events with normal business context

Governance Parameters

The following table provides a quick comparison of the GRC framework of Gartner, cyber-security framework of NIST and Aegify frameworks.

NIST	Gartner	Aegify
Identify	IT Asset Repository;	Business Context, Application Context, Sytem Context, Risk Context, Assets, Vulnerabilities, Time, User, Data
Protect	Controls and Policy Mapping; Policy distribution and attestation; Automated General Computer Control collection	Ready to use security and privacy polices; built-in policy editor, Harmonized Controls, events, systems and applications, data and user towards regulatory controls

Detect	IT Control Self Assessment and Measurement ; IT Risk evaluation; IT compliance dashboard	Automated security, risk, and compliance assessments (self or by Managed Service Providers) and vulnerabilities views (CVE & CWE), Dashboard and Reports, multi-dimensional data analysis, and 7-D data normalization (refer details below)
Respond Recover	Remediation and Exception management	Remediation measures; Review by Auditors/Managed Service Providers

Aegify GRC Framework

Compliance Framework:

Governance - Governance in Aegify context is the culture, values, mission, structure and layers of policies, processes and measures by which organizations are directed and controlled. Governance, in this context, includes, but is not limited to the activities of the Board, as governance bodies at various levels throughout the organization also play a critical role. The tone that is set, followed and communicated at the top is critical to success. As part of effective governance, Aegify has built-in ready-to-use safety and security policies with a built-in policy editor to customize the policies, if required to suit the organization’s requirements. The policies cover specific to HIPAA/HITECH, PCI DSS, SANS20, ISO27K, and other standards and regulations. The aegify tool was built on an architecture framework that allows plugging into the tool any regulation/standard for compliance assessment quickly. The controls associated with any standard or regulations could quickly and easily be incorporated into the tool. The reporting and dashboard features provide quick ways of viewing and analysing the security, risk, and compliance from multiple perspectives – from a regulatory point of view, from a risk point of view and from an assets point of view. Drilling down from a control perspective, the user can view the different assets that are not compliant with ready to use measures to fix the non-compliant issues. The what-if analysis module of Aegify helps in analyzing different risk scenarios helping the organization to prioritize critical assets in ensuring privacy and security.

Compliance - Compliance is the act of adhering to, and the ability to demonstrate adherence to, mandated requirements defined by laws and regulations, as well as voluntary requirements resulting from contractual obligations and internal policies. Aegify SecureGRC is a cloud-based Compliance Manager, making it extremely easy to assess the compliance status of business organizations - small, medium, and large - to various compliance regulations and standards. Aegify SecureGRC streamlines effective compliance management. Generates compliance gap reports with complete remediation guidance to help continuously monitor your compliance status through real-time dashboards that reflect your organization’s current status based on context-specific changes. Built on a framework approach, Aegify SecureGRC provides an effective infrastructure to verify compliance to any regulation or standard and could easily be customized to meet specific requirements of a customer.

Harmonization of controls under various regulations/standards - Harmonized controls helps organizations quickly map to different regulations and standards in one shot simplifying the rigor of assessing under different compliance requirements through automated mapping of related controls.

Risk - Risk, in this context, is the measure of the likelihood of something happening that will have an effect on achieving objectives; most importantly, but not exclusively, an adverse effect. Thus, Risk Management is the systematic application of processes and structures that enable an organization to identify, evaluate, analyze, optimize, monitor, improve, or transfer risk while communicating risk and

risk decisions to stakeholders. The overriding goal of risk management is to realize potential opportunities while managing adverse effects of risk. Risk analysis and management are mandated by every security standard and regulation to identify potential risks to organizations that deploy IT assets. Aegify's risk module is intensive. It helps you automate risk management using built-in expert system leveraging best-practice inputs from standards such as NIST, ISO, and OCTAVE among others. You could define the asset-based risk factors and the relationships among those factors - threat, vulnerability, impact, likelihood, and predisposing conditions. It minimizes your risks significantly through automated vulnerability management lifecycle, scanning for more than 31,800 vulnerabilities and running over 92,000 checks across your network. It integrates with Aegify Security Posture and Compliance Management helping you calculate your risks, based on your compliance and security posture and minimizes your security risks with proactive, customizable risk management measures such as exposure, economic, consequence, legal, and risk likelihood. The built-in risk filters helps you quickly generate extensive risk reports.

Security - Security Posture Management is the art of monitoring and managing the security status by orchestrating process-people-technological resources towards achieving the business security objectives.

This involves identifying business critical IT assets, evaluating their risks based on vulnerabilities and the impact of potential threats, for initiating appropriate measures towards ensuring Confidentiality, Integrity, and Availability of information assets.

Unified and Integrated Security, Risk, and Compliance Management

Top-down strategic perspectives meets with bottoms-up security, risk, and compliance best practices using Aegify.

Against silos of solutions offered in the market for security, risk, and compliance, Aegify provides an integrated and seamlessly unified solution through its **Aegify Scanner** that identifies the vulnerabilities in the tech infrastructure – hardware and software and maps the scan vulnerability results to the security, risk and compliance controls of various regulations and standards, **Aegify compliance manager** that assesses through auto mapping the scan results to the compliance conformity requirements through the controls and based on specific business contexts provides a risk analysis framework to mitigate the risks through the appropriate remedial measures through **Aegify Risk Manager**.

Key components of Aegify

Aegify offers a comprehensive suite of solutions for compliance, risk and security management in simple steps.

Security Posture Management (SPM)

Security Management is the art of securing the business assets for their confidentiality, Integrity, and Availability to ensure business continuity through planning, organizing, controlling, leading and directing processes, people, and technological resources in the organization to achieve its business security objectives. Various regulations such as HIPAA/HITECH, FISMA or Standards such as PCI or ISO 27K define the security controls in controlling the security management effectively. HIPAA categorizes these controls into Physical, Administrative, and Technical Safeguards. FISMA categorizes the controls into Management, Operational and Technical. All controls essentially cover People, Process, and Technology.

The task of managing Security is complex, as Security is in a fluid state of uncertainty at any point in time. When you think that your security controls are in place and you are secure, a small slip by people, process or technology in a business critical asset is enough to slide your security level from very high to very low. And if a breach happens when somewhere in your IT infrastructure there is an unplugged gaping hole and that is exploited by ever watchful cyber attackers, you have all the hell lose, with federal authorities on your back, your reputation in question, penalties threatening you, and your business continuity is affected. There are over 28,000 such security gaps identified and documented as 'vulnerabilities'.

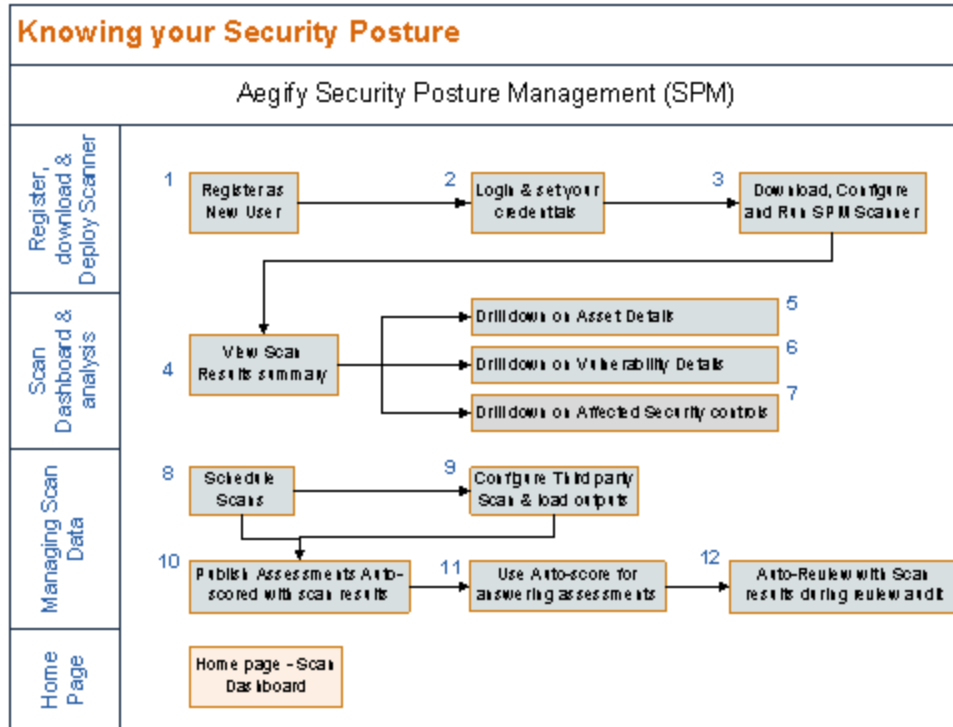
Information systems, unfortunately, are inherently insecure. Technical solutions are an essential but only one portion in the holistic approach to security. You must understand your unique threat environment given your area of business operations through an effective risk management methodology. This involves discovering all your authorized assets in your infrastructure. With multiple devices used by people in your network, at any point in time it is extremely difficult to ascertain your current inventory of assets.

Therefore continuous asset identification, asset classification, criticality of such assets in your business, mapping the risk from low to high, monitoring of threats on a continuing basis, analyzing the consequential impact of such threats to your business continuity, discovering existing and new vulnerabilities, finding a solution to fix such vulnerabilities, fixing the solution, and continuing to monitor is a never-ending cycle. You need a Security measurement meter that will keep a tab on your security level monitoring your assets, risks, vulnerabilities, threats, providing your effective solution instantly in fixing issues when your security level slides down the security-meter.

Today the information security market offers silos of solutions that do not integrate with each other to provide you a holistic view.

Security Posture Management is the art of managing the security status to achieve the business security objectives by identifying critical IT business assets, evaluating their risks based on vulnerabilities and the impact of potential threat-likelihood, and initiating appropriate remedial measures to ensure Confidentiality, Integrity, and Availability of information assets by planning, organizing, controlling, and directing process-people-technological resources.

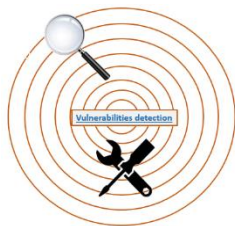
Simple steps in assessing the security posture of an organization is illustrated below:



Guide

Follow the flow in this diagram for assessing and managing your security posture. The row-headers indicate the key resources and the steps involved within each of these Scan steps. Click on a node in the workflow to view and understand more.

Perimeter Scanning



As part of vulnerability assessment Aegify scanner allows scanning of external IP addresses (Perimeter)

Aegify scanner gives you the following distinct features that other web scanners do not offer:

Browser Emulation Scanning Technology (BEST) - Browser-based scanning of client-side Web applications to find vulnerabilities in deployed and running web applications such as JavaScript, AJAX, and Flash

Web Application Pass-Through Scanning- Uses current vulnerabilities to scan and accurately report on unaddressed vulnerabilities and web applications including third-party applications exposures deep in the network, providing a more accurate and complete report.

Batched Scanning- Reduces scan times and allows customers to target specific and mission critical addresses.

Content Scanning- Scans Databases and applications for specific content such as credit card and social security numbers, ensuring personally identifiable information is not visible to hackers.

Operating System Scanning

Aegify scanners scan for the following vulnerabilities and other vulnerabilities as and when they are identified:

- Command Execution

- Parameter Injection
- SQL Injection
- Cross-Site Scripting
- Directory Traversal
- Abnormal Input
- Parameter Overflow/ Buffer Overflow
- Parameter Addition
- Path Manipulation/ Path Truncation
- Character Encoding
- MS-DOS 8.3 Short Filename
- Character Stripping
- Site Search
- Application Mapping
- Crawl
- Automatic Form-Filling
- SSL Support
- Proxy Support
- Client Certificate Support
- State Management
- Directory Enumeration
- Web Server Assessment
- HTTP Compliance
- WebDAV Compliance
- SSL Strength
- Certificate Analysis
- Content Investigation
- Spam Gateway Detection
- Client-Side Pricing
- Sensitive Developer Comments
- Web Server/ Web Package Identification
- Absolute Path Detection
- Error Message Identification Permissions
- Permissions Assessment
- Known Attacks
- Session Hijacking

Aegify Compliance Manager

Aegify Compliance features include:

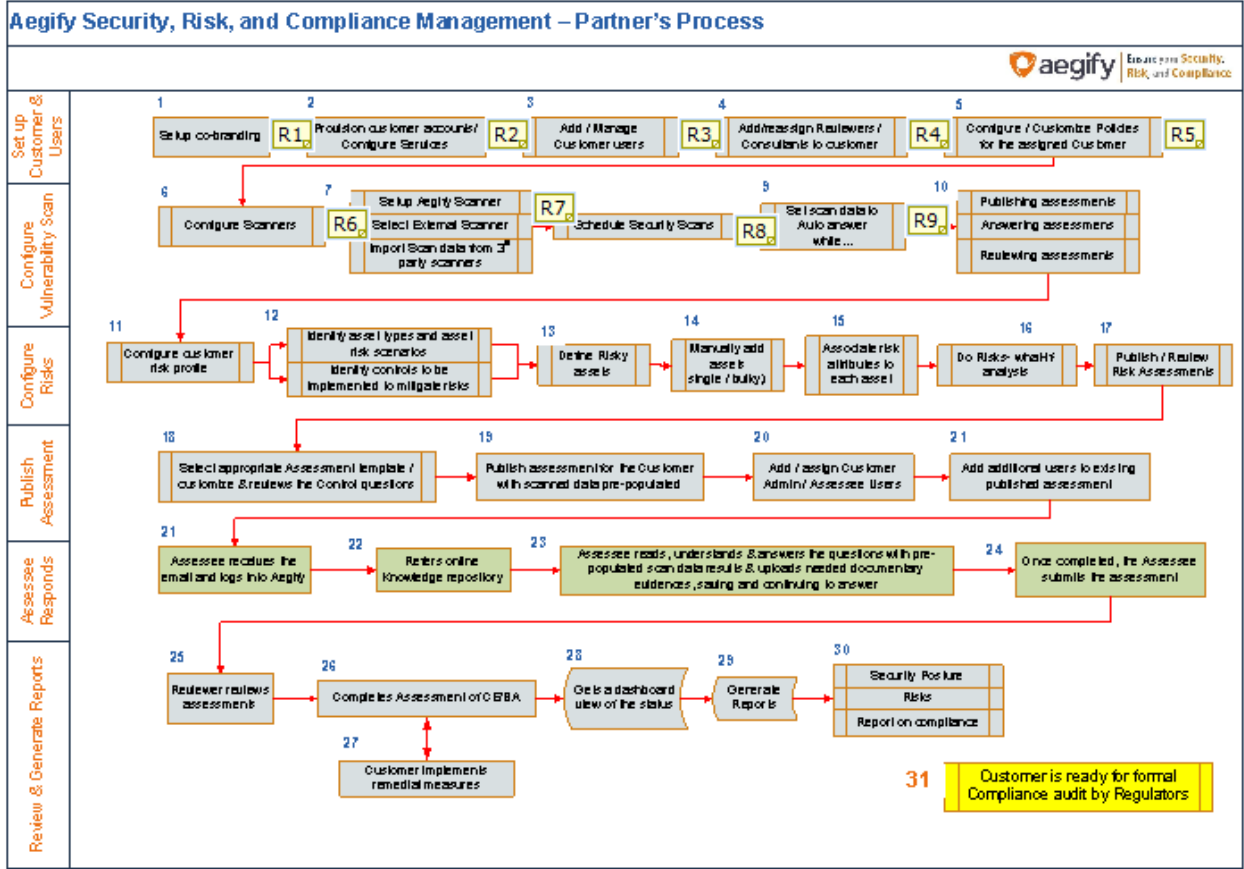
- Ready-to-use compliance controls in HIPAA/HITECH, PCI DSS, ISO 27K, FISMA and Sox also facilitating easy fit of any regulation or standard to assess compliance status.
- Easily customizable to meet enterprise-specific requirements with flexibility in deployment
- Easy customization to meet enterprise-specific requirements and provide flexibility in deployment.

- Helps identify compliance gaps through vulnerability scan and auto-maps scan results to compliance assessments.
- Provides ready-to-use built-in policies, procedures, and assessment templates that can easily be customized.
- Features quick access to documentation and evidence from central repository for pre/post audits.
- Facilitates management of Business Associate compliance.
- Provides security within SaS 70 Type II secure data center.
- Generates significant cost savings by requiring no investments in hardware and software.
- Helps secure federal EMR grants with proactive risk measures and helps assess risks through a systematic algorithmic analysis, fine-tuned to regulatory requirements. Customization of configurable risk parameters (exposure, economic risk, consequence, and legal exposure) for different authority documents, based on risk likelihood and through an easy interface.
- Ensuring Compliance to HIPAA/HITECH, for instance is a simple 5-step process as illustrated below:

Five Steps for Omnibus Rule Compliance



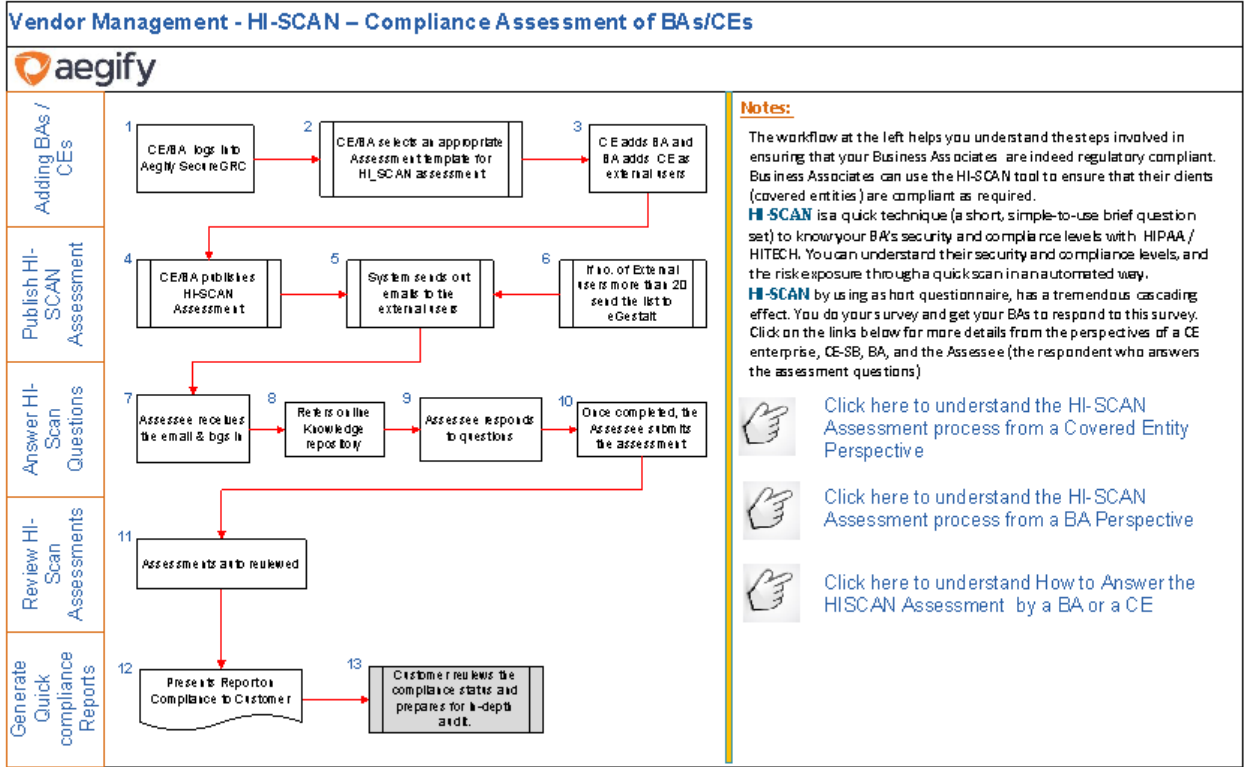
The compliance process is illustrated below:



Vendor Management

Section 13401 of subtitle D (Privacy) of the HITECH Act (42 USC 17931) states that "the additional requirements of this title that related to security and that are made applicable with respect to Covered Entities shall also be applicable to such a Business Associate and shall be incorporated into the business associate agreement between the business associate and the covered entity" [Public Law 111-5, p 260]. In addition, penalties that apply to Covered Entities also will apply to Business Associates for non-compliance with the provisions of the Security Rule.

- Aegify offers a quick litmus Assessment test through a set of short (25 questions) risk assessment to quickly assess the level of compliance of your business partners. It’s a kind of pH measure of information security.
- Your Business Associates could include offsite backup facility, transcription services, billing services, remote managed services, IT Service Provider, third party administrators that assist health plans with claims processing, pharmacy benefit managers, CPA/Attorney/law firms who have access to PHI, and Consultants that perform utilization review for a hospital.
- HI-SCAN is a quick technique to let you know the extent of compliance of your BAs to HIPAA / HITECH regulatory requirements. You can understand their security and compliance levels, the risk exposure through a quick scan in an automated way.
- The BA Assessment workflow using HI-SCAN tool is as follows:



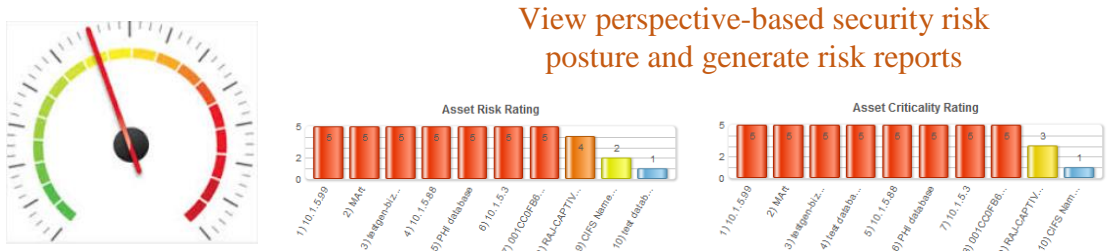
Aegify Risk Manager

Automate Business Risk Management with Aegify Risk Manager in four simple steps:

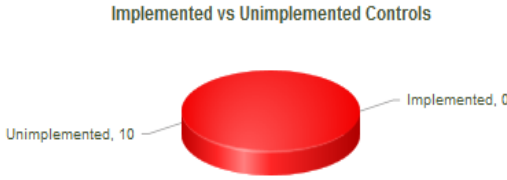
1 Manage Assets



2 Configure & Assess Risk Levels, View Reports

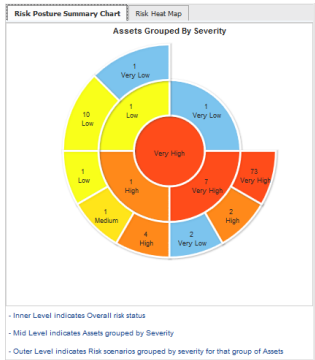


3 Assess Compliance



- Review risks from published and responded assessment.
- Generate risk reports.

4 Do What-if Analysis



- Simulate risk scenarios and view security posture at different risk settings.
- Prioritize remedial actions.
- Stay Secure, Risk-free, and Compliant with Aegify.

Meaningful Use Grants



To qualify for a meaningful-use grant—for which the U.S. Department of Health and Human Services has set aside a \$28 billion stimulus fund—healthcare organizations must conduct a mandatory security risk analysis in accordance with the requirements under HIPAA regulation 45 CFR 164.308(a)(1).

As part of the security risk analysis, you are required to identify security and compliance deficiencies through a risk assessment process, and then generate a detailed meaningful use report that can be submitted to the federal government to receive the stimulus grant money.

Aegify can help you quickly generate the meaningful-use report by scanning your network; discovering all HIPAA critical assets and their security vulnerabilities; generating a detailed HIPAA compliance and security gap report; and providing remediation guidance to fix any gaps found.

The first stage of the Electronic Health Record (EHR) funding deadline expired as of February 28th, 2012 and was focused on data capture and sharing. The second stage for 2014 is focused on advanced clinical processes. The third stage in 2016 focuses on improved outcomes.

The incentives, which ranged between \$44K and \$63K for small-to-medium Covered Entities and \$2M for hospitals, are gradually being lowered, starting from 2013. However, meaningful use requirements need to be renewed annually, and **disincentives start kicking in during 2015 and 2016**. There will thus be an ongoing need to perform and maintain meaningful use analysis every year.²

Meaningful use of EHR achieves the following objectives:

- Quality, safety, efficiency in health records, and reduction in health disparities

- Care coordination and public health
- Privacy and security of Patient Health Information (PHI)
- Quality research data on health systems

The meaningful use report—generated with a single click in Aegify—portrays the results of a risk analysis **based on NIST 800-30 methodology** while also taking into consideration the following:

- Identification of all IT assets that capture, process, store or transmit PHI.
- Compliance assessment of HIPAA compliance requirements, including Security Rule controls.
- Security scanning of all PHI critical assets.
- Risk management to assess the overall business risk and provide relevant guidance on mitigating organizational risk.

The Aegify Meaningful Use Bundle includes Aegify SecureGRC for HIPAA compliance management, Aegify SPM for Security Posture Management and Aegify Risk Manager for effective risk management.

Aegify simplifies all of these processes through automation and interlinking of security, privacy, regulatory/standard controls. The solution leverages one convenient bundle that performs all tasks for all your HIPAA compliance and Meaningful Use needs.

Automated SRC Processes

Automation of SRC Governance process makes a big difference —

Automation of processes takes away the rigor of the routine and the mundane tasks. Automation is so ubiquitous all around us, that in many cases, we don't even recognize it. Security, Risk, and Compliance are ongoing requirements, and given the increasing cyber-threats and the challenges to effectively address them, automation helps in ensuring routine checks and in preventing known security issues by automatically monitoring security, risk and compliance issues on a routine automated basis.

Effective governance demands that an organization's business objectives are realized by conforming to established regulations and standards and be able to demonstrate conformance quickly through documentary evidence. Governance could become a night mare as there are multiple regulatory requirements that must be met; organizations have this difficult task of ensuring the organization's practices are indeed in conformance with regulatory policy objectives and the controls that help ensuring that they stay on track. The negative effects of bad governance are many fundamentally affecting the core business whether they be in terms of brand-loss or the civil and criminal penalties significantly draining out the organizations critical resources.

Aegify's context specific analysis and multi-dimensional Data analysis helps in prioritizing the risks and critical controls by which protection measures implemented could be most effective. In addition, the harmonized controls helps organizations quickly map to different regulations and standards in one shot simplifying the rigor of assessing under different compliance requirements through automated mapping of related controls.

Aegify simplifies all of these processes through automation and interlinking of security, risk, privacy, and regulatory/standard controls. The solution leverages one convenient bundle that performs all tasks for all your HIPAA compliance and Meaningful Use needs. The 7-D multi-dimensional data analysis and the

Aegify GRC framework is unique and significant as it simplifies security and compliance across multiple regulations and standards.

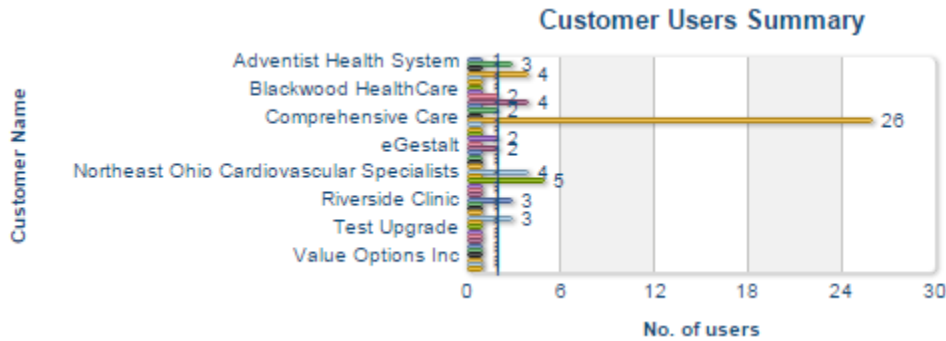
Aegify automation features

- Harmonization of controls across regulations and standards
- Aegify Scans for vulnerabilities and configurations auto-populates assessment responses with scanned data
- Automates the assessment review process for Auditors/Managed Service Providers
- Based on identified vulnerabilities remediation measures recommended for immediate fixing
- Scanner auto detects new assets as they are plugged into the network
- Ready to use policies that are easily customizable
- Relevant policy documents are readily mapped to regulatory controls and standards
- Facility to upload documentary evidence of compliance
- Provides automatic regulatory updates
- Security data automatically mapped to seven data dimensions for meaningful scrutiny.
- Auto-scans the IT infrastructure for vulnerabilities
- Provides comprehensive automated multiple perspectives – vulnerabilities, risks and controls.

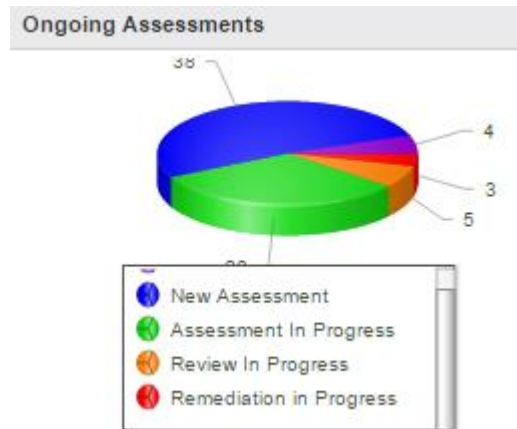
Extensive Reports and dashboard views for quick remedial action and audit preparedness with What-if-Analysis

Aegify dashboards and reports are intuitive with clear call-to-action on remedial measures to be taken for plugging the SRC gaps. These views and reports address different stakeholders, such as MSSPs who could generate admin reports. A sample dashboard is displayed:

Assessment reports



, or a dashboard



view of the ongoing assessments

Various compliance assessment reports include customer assessment summary, compliance status by regulation, Report on Compliance.

Asset Management Reports

Asset Management reports include asset view, vulnerability view, affected controls view, vulnerability remediation report, and configuration checks view and advanced Security Posture Management Reports.

Risk Reports

Risk reports provide perspective reports on risky assets, most effective controls, and top risk scenarios.

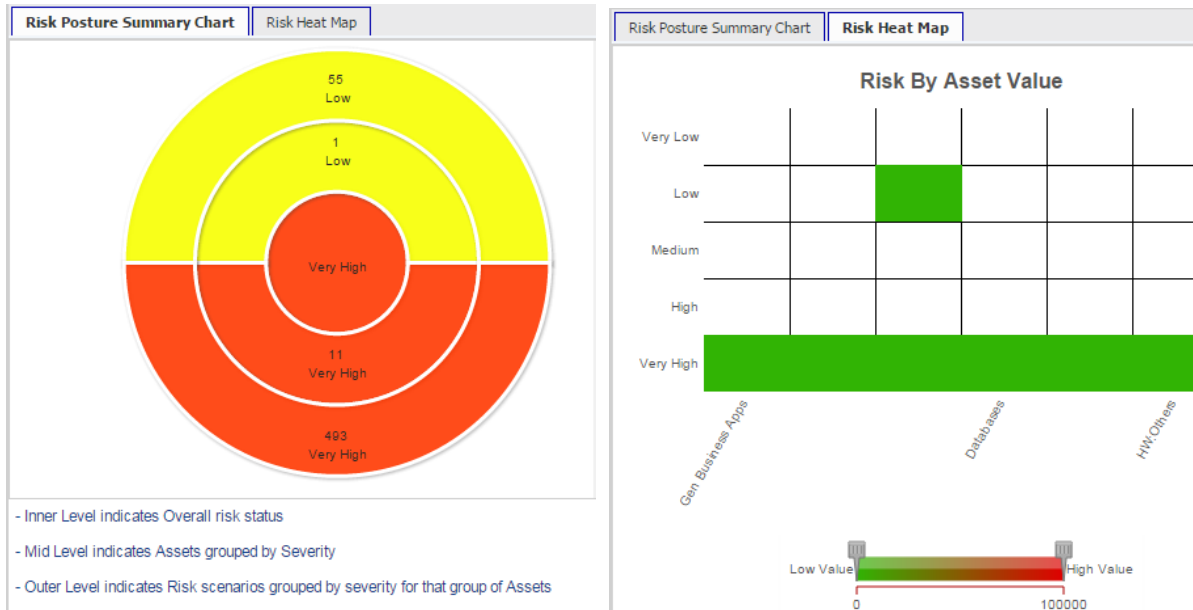
What-if-Analysis

What-If Analysis gives a powerful simulation model to assess the impact on security and compliance levels for a selected customer by defining the count of assets to be evaluated and the perspective – in terms of controls and risk scenarios.

Security Posture and Risk Heat Map Reports

Various applicable controls listed in the left panel could be selected the check the control to indicate whether the control is implemented and to instantly display the risk scenario, the number assets impacted by the control and the percentage of controls scored. After selecting or deselecting the controls that are implemented, clicking 'Calculate' displays the extent to which the selected customer is compliant through the pie chart on the right. The multi-level pie chart shows three layers: The inner

most circle shows the severity of the overall risk status; the middle circle shows the assets grouped by severity; the outer circle displays the risk scenarios grouped by the severity for the group of assets.



Selecting the heat map tab to the right of the multi-level pie chart shows the risk by asset value for the different assets for which the compliance controls have been implemented.

Exclusive Partner Portal

An exclusive partner portal provides rich resources to partners for marketing collaterals, Lead generation tools, setting up compliance policies, and risk profile for their customers, white papers, knowledge base and a dedicated customer support to address queries and support to the partners. With a single sign-on facility, partners can access the partner portal resources from the aegify application portal.

Distinct features of Aegify Summarized

Aegify offers:


- Complete integration and unification of Security, Risk and Compliance Management through a single Platform.
- Built in Expert-system to unify and seamlessly integrate Security, Risk and Compliance Information data using a single dashboard (and report(s)).
- Providing security, Risk and Compliance GAP reports with complete remediation guidance with time estimates for fixing the problem.
- Complete Policy and Contract Management Portal for managing documents, version control, audit trail and mapping to GRC compliance controls
- Auto-answering of HIPAA assessments using automated asset discovery and Security Scanning
- Ability to proactively manage Security, Risk and Compliance status of all the business associates and sub-contractors/vendors

- Complete HIPAA compliance solution with complete HIPAA questionnaire, integrated Security Scanning and Security Risk Analysis capabilities
- Support for meaningful use attestation process with 1-click reports for meeting Stage 1 and Stage 2 requirements for Security risk analysis
- HIPAA Security, Risk and Compliance GAP reports with Complete remediation guidance with time estimates for fixing the problem
- Pre-Audits, Audits and Continuous monitoring of HIPAA Security, Risk and Compliance Status of CE's, BA's and Subcontractors/Bas
- HIPAA Training Integration for Awareness training of employees and vendors
- Complete knowledge Base with HIPAA Policies, Contracts, Procedures, Agreements, Industry Best Practices and Complete Implementation guidance
- Real-time Dashboard with customizable Reports
- HIPAA regulation updates every quarter
- Ability to manage HIPAA Security, Risk and Compliance status of all the business associates and sub-contractors/vendors
- Real-time Dashboard with HIPAA status for all the Bas, subcontractors and Vendors
- Comprehensive HIPAA omnibus questionnaire for CE's and Bas
- Support basic questionnaire for Covered Entities and Business Associates
- Support for multiple regulations/standards such as HIPAA, PCI, FISMA, SANS20, SOC2 etc.
- Harmonization of controls across multiple regulations/standards - Do it once and reflect the status across regulations
- Auto-answering of HIPAA assessments using automated asset discovery and Security Scanning
- Complete Policy and Contract Management Portal for managing documents, version control, audit trail and mapping to HIPAA compliance controls
- Complete HIPAA remediation guidance with training, policies, contracts and best practices and implementation guidelines
- Integrated Security and Vulnerability Scanning Solution
- Cloud based remote deployment and management model
- Automated Mapping of Security Controls to HIPAA compliance regulations using an expert systems framework
- Ability to import results from industry standard scanners
- Complete HIPAA Risk Assessment support for single location to multi-location large enterprises
- Basic HIPAA Risk assessment for Security Risk Analysis
- Support NIST, ISO, OCTAVE and ISO risk management frameworks
- Unified Risk - takes into account both security and compliance assessments
- Support multiple pricing and deployment models suitable for deploying in small businesses to large enterprises; Scales from 1 User/Location to 100s of users and locations; 10s of assets to 1000's of assets can discovered and scanned.
- Multiple Deployment models - Hierarchical with a roll-up and location specific views or a Centralized deployment model

- Extensible Platform that has the ability to import results from industry standard scanning tools, compliance tools to unify and integrate the results
- Cloud based deployment, management and monitoring model that doesn't require on-site presence for managing multiple locations

[Download the comparison chart](#) for a comparative analysis of Aegify features vis-à-vis features offered by various products in the market.



 is a world-class, innovation driven leader of cloud-computing business solutions for information security, risk, and IT-GRC management. Headquartered in Cupertino, California, Aegify Inc., (earlier registered as eGestalt Technologies Inc.,) has offices through the US, Asia-Pacific and Middle East. To learn more about Security, risk, and compliance solutions from eGeAegify and how we can help you protect your healthcare-related organization, visit <http://www.aegify.com>, call us at +1-(408)-689-2586, or email at sales@aegify.com.

To learn more about how the Aegify Security Posture Management, Aegify SecureGRC Compliance Management tools, and Aegify Risk Manager can help you protect your organization, visit www.aegify.com, call **+1 (408)-689-2586**, or email sales@aegify.com.

