

**SOLUTION BRIEF:****ALERT LOGIC SECURITY COMPLIANCE**

Compliance is a challenge for many organizations as stretched security and IT staff struggle to keep up with requirements that seem to constantly evolve. Regulators continue to impose compliance rules to protect organizations, individuals and industry groups from data breaches and data loss. One result of this is that companies are allocating 14.3% on average of their IT budget to compliance spending. And, the cost of non-compliance can be 2.7 times higher than the cost of compliance due to business disruption, revenue losses, fines, and settlement costs.<sup>1</sup>

***THE COST BURDEN IS INCREASED WITH THE NEED TO FIND AND RETAIN DEDICATED PROFESSIONAL STAFF, AND TO IMPLEMENT TECHNOLOGIES TO CURTAIL RISK.***

It's time think differently. The traditional way has organizations increasing their security spend each year yet they are not getting closer to achieving the compliance outcomes. Traditional security tools and point products continue generate a myriad of alerts which require highly skilled expertise which is in short supply in order to get value. Organizations want a simpler way meet compliance across multiple regulations without having to hire and train additional staff.

**WHY ALERT LOGIC FOR COMPLIANCE?**

- We help organizations achieve compliance with minimal disruption with a security and threat management platform and expert staff support for any environment
- Our experts will filter out the noise and investigate and respond to incidents that could lead to a business being out of compliance
- We provide services 24 hours a day, every day of the year—offloading the high costs of in-house security staff
- Our SOC provides security experts who will review incidents and provide additional context and remediation actions based on knowledge gathered from thousands of incidents
- We work personally with each customer to provide personal notifications. Our analysts call, text or email you within 15 minutes of high- and critical-priority attacks

<sup>1</sup> Ponemon Institute and Globalscape *The True Cost of Compliance with Data Protection Regulations*

**2.7X**  
higher cost for  
non-compliance than  
the cost of compliance

**14.3%**  
average of a companies  
IT budget allocated to  
compliance

## ALERT LOGIC SECURITY COMPLIANCE BENEFITS

- Quickly understand state of compliance without hiring new staff
- Audit-ready reporting that helps IT staff stay one step ahead of requirements, mandates and auditors
- Improved security posture, reduced attack surface and risk of data breach
- Get informed advice and remediation steps from our security experts
- Streamlined governance processes, and build compliance controls directly into IT processes
- Build trust with your stakeholders, customers and prospects by providing proof to stakeholders who require it
- Take the lead over competitors by offering proof of compliance where your prospects are likely to appreciate your above-and-beyond approach to business precautions

***“Using Alert Logic’s managed threat defense solution in conjunction with our other security measures, helped us to demonstrate compliance with the PCI Data Security Standard and pass the audit”***

***Wyman Lewis, Director of Information Security, GSI Commerce***



***“It made it very easy for us to check the boxes and make sure we are covered without having to invest a whole lot in new personnel,”***

***Bill Thornton, Vice President, Tango***



# ALERT LOGIC SOLUTIONS COMPLIANCE MAPPING

OFFERINGS	PCI DSS 3.2	HIPAA & HITECH	SOC 2 (TSP 100)
<p><b>Alert Logic Professional Includes Essentials</b>  <i>24/7 Managed Threat Detection and Incident Management</i></p> <ul style="list-style-type: none"> <li>- 24/7 Incident Monitoring &amp; Management</li> <li>- Security Analytics &amp; Threat Intelligence</li> <li>- Log Collection and Monitoring</li> <li>- Intrusion Detection</li> <li>- Security Event Insights and Analysis</li> <li>- Office 365 Log Collection &amp; Search</li> <li>- Cloud Vendor Security Integrations</li> <li>- AWS User Behavior Anomaly Detection</li> <li>- Anti-Virus Integration</li> </ul>	<p><b>10.1</b> - Implement audit trails</p> <p><b>10.2</b> - Automated audit trails</p> <p><b>10.3</b> - Capture audit trails</p> <p><b>10.5</b> - Secure logs</p> <p><b>10.6</b> - Review logs</p> <p><b>10.7</b> - Maintain logs online</p> <p><b>10.7</b> - Retain audit trail</p> <p><b>10.8.1</b> - Respond to failures of critical security controls</p> <p><b>11.4</b> - Use intrusion-detection and/or intrusion-prevention techniques</p> <p><b>12.10.1</b> - Implement an incident response plan</p>	<p><b>164.308 (a)(1)(ii)(B)</b> - Risk Management</p> <p><b>164.308 (a)(1)(ii)(D)</b> - Information System Activity</p> <p><b>164.308 (a)(4)(i)</b> - Information Access Management</p> <p><b>164.308 (a)(5)(ii)(B)</b> - Protection from Malicious Software</p> <p><b>164.308 (a)(5)(ii)(C)</b> - Login Monitoring</p> <p><b>164.308 (a)(6)(ii)</b> - Response &amp; Reporting</p> <p><b>164.312 (a)</b> - Access Control</p> <p><b>164.312 (b)</b> - Audit Controls</p>	<p><b>CC 6.2</b> - User Registration</p> <p><b>CC 6.3</b> - Access Modification</p> <p><b>CC 7.2</b> - Security Event and Anomaly Detection</p> <p><b>CC 7.3</b> - Incident Detection and Response</p>
<p><b>Alert Logic Essentials</b>  <i>Vulnerability &amp; Asset Visibility</i></p> <ul style="list-style-type: none"> <li>- Asset Discovery</li> <li>- Vulnerability Scanning</li> <li>- Cloud Configuration Checks</li> <li>- Extended Endpoint Protection</li> <li>- Threat Risk Index</li> <li>- Compliance Scanning and Reporting</li> </ul>	<p><b>6.1</b> - Identify vulnerabilities</p> <p><b>11.2</b> - Perform network vulnerability scans by an ASV (Includes 11.2.1, 11.2.2 and 11.2.3)</p>	<p><b>164.308 (a)(1)</b> - Security Management Process</p> <p><b>164.308 (a)(1)(i)(A)</b> - Risk Analysis</p>	<p><b>CC 3.2</b> - Risk Identification</p> <p><b>CC 6.6</b> - External Threats</p> <p><b>CC 6.8</b> - Unauthorized and Malicious Code Protection</p> <p><b>CC 7.1</b> - Vulnerability Management</p>
<p><b>Alert Logic Enterprise Includes Professional</b>  <i>Managed Web Application Firewall and Assigned SOC Analyst with Threat Hunting</i></p> <ul style="list-style-type: none"> <li>- Always-on Managed WAF Defense</li> <li>- Assigned SOC Analyst</li> <li>- Controlled Threat Hunting</li> <li>- Dark Web Scanning</li> </ul>			

## ALERT LOGIC SOLUTIONS COMPLIANCE MAPPING (CONT.)

	GDPR	SOX 404
<p><b>Alert Logic Professional Includes Essentials</b>  <i>24/7 Managed Threat Detection and Incident Management</i></p> <ul style="list-style-type: none"> <li>- 24/7 Incident Monitoring &amp; Management</li> <li>- Security Analytics &amp; Threat Intelligence</li> <li>- Log Collection and Monitoring</li> <li>- Intrusion Detection</li> <li>- Security Event Insights and Analysis</li> <li>- Office 365 Log Collection &amp; Search</li> <li>- Cloud Vendor Security Integrations</li> <li>- AWS User Behavior Anomaly Detection</li> <li>- Anti-Virus Integration</li> </ul>	<p><b>Article 34</b> - Communication of a personal data breach</p>	<p><b>DS 5.5</b> - Security Testing, Surveillance and Monitoring</p> <p><b>DS 5.6</b> - Security Incident Definition</p> <p><b>DS 13.3</b> - IT Infrastructure Monitoring</p>
<p><b>Alert Logic Essentials</b>  <i>Vulnerability &amp; Asset Visibility</i></p> <ul style="list-style-type: none"> <li>- Asset Discovery</li> <li>- Vulnerability Scanning</li> <li>- Cloud Configuration Checks</li> <li>- Extended Endpoint Protection</li> <li>- Threat Risk Index</li> <li>- Compliance Scanning and Reporting</li> </ul>	<p><b>Article 24</b> - Responsibility of the controller</p> <p><b>Article 25</b> - Data protection by design and by default</p> <p><b>Article 32</b> - Security of processing</p> <p><b>Article 35</b> - Data protection impact assessment</p>	<p><b>DS 5.9</b> - Malicious Software Prevention, Detection and Correction</p>
<p><b>Alert Logic Enterprise Includes Professional</b>  <i>Managed Web Application Firewall and Assigned SOC Analyst with Threat Hunting</i></p> <ul style="list-style-type: none"> <li>- Always-on Managed WAF Defense</li> <li>- Assigned SOC Analyst</li> <li>- Controlled Threat Hunting</li> <li>- Dark Web Scanning</li> </ul>		

## ALERT LOGIC SOLUTIONS COMPLIANCE MAPPING (CONT.)

OFFERINGS	ISO 27001/27002	NIST 800-171	NIST 800-53
<p><b>Alert Logic Professional</b> Includes Essentials <i>24/7 Managed Threat Detection and Incident Management</i></p> <ul style="list-style-type: none"> <li>- 24/7 Incident Monitoring &amp; Management</li> <li>- Security Analytics &amp; Threat Intelligence</li> <li>- Log Collection and Monitoring</li> <li>- Intrusion Detection</li> <li>- Security Event Insights and Analysis</li> <li>- Office 365 Log Collection &amp; Search</li> <li>- Cloud Vendor Security Integrations</li> <li>- AWS User Behavior Anomaly Detection</li> <li>- Anti-Virus Integration</li> </ul>	<p><b>12.2</b> - Protection from malware.</p> <p><b>12.4</b> - Logging and monitoring.</p> <p><b>16.1</b> - Management of information security incidents and improvements</p>	<p><b>3.5</b> - Identification and Authentication</p> <p><b>3.6</b> - Incident Response</p>	<p><b>CA-2</b> Security Assessments</p> <p><b>CA-3</b> Information System Connections</p> <p><b>CA-7</b> Continuous Monitoring</p> <p><b>IR-5</b> Incident Monitoring</p> <p><b>IR-6</b> Incident Reporting</p> <p><b>IR-7</b> Incident Response Assistance</p> <p><b>SC-7</b> Boundary Protection</p> <p><b>SI-3</b> Intrusion Detection Tools and Techniques</p> <p><b>SI-4</b> The organization employs tools and techniques to monitor events on the information system, detect attacks, and provide identification of unauthorized use of the system</p> <p><b>SI-5</b> Security Alerts And Advisories</p> <p><b>SI-7</b> Software And Information Integrity</p>
<p><b>Alert Logic Essentials</b> <i>Vulnerability &amp; Asset Visibility</i></p> <ul style="list-style-type: none"> <li>- Asset Discovery</li> <li>- Vulnerability Scanning</li> <li>- Cloud Configuration Checks</li> <li>- Extended Endpoint Protection</li> <li>- Threat Risk Index</li> <li>- Compliance Scanning and Reporting</li> </ul>	<p><b>8.1</b> - Responsibility for assets</p> <p><b>12.6</b> - Technical vulnerability management</p>	<p><b>3.1</b> - Access Control</p> <p><b>3.3</b> - Audit and Accountability</p> <p><b>3.4</b> - Configuration Management</p> <p><b>3.11</b> - Risk Assessment</p> <p><b>3.12</b> - Security Assessment</p> <p><b>3.13</b> - System and Communications Protection</p> <p><b>3.14</b> - System and Information Integrity</p>	<p><b>RA-3</b> Risk Assessment</p> <p><b>RA-5</b> Vulnerability Scanning</p>
<p><b>Alert Logic Enterprise</b> Includes Professional <i>Managed Web Application Firewall and Assigned SOC Analyst with Threat Hunting</i></p> <ul style="list-style-type: none"> <li>- Always-on Managed WAF Defense</li> <li>- Assigned SOC Analyst</li> <li>- Controlled Threat Hunting</li> <li>- Dark Web Scanning</li> </ul>			