MANAGED GOVERNANCE AND COMPLIANCE

Helping You to Remain Compliant Between Audits

Thefinancialbenefitsandagilitygainedbyutilizingthepublic cloudiswellworththereturnandrequiresnewskills,software andmanagementtomaintainregulatorycomplianceswithin your organization.

Teams are able to spin up unlimited number of resources within moments and deploy new applications very easily compared to traditional IT methods. Without the proper governance in place organizations can be exposed to security vulnerabilities and potentially compromise confidential information.

2nd Watch's Managed Governance and Compliance services are designed to help your Chief Security and Compliance Officers (CISCO) maintain visibility and control of what is happening in your public cloud environment at all times.

We start by documenting and mapping out your regulatory compliance requirements, as related to your industry, your business, and/or any other specialized or classified concerns. Following this initial consultation, 2nd Watch will run a comprehensive assessment of your entire cloud infrastructure in order to determine just how closely aligned your company is to the regulatory guidelines applicable to your organization.

Clients receive a detailed report containing the entire, in-depth analysis, including identification of known vulnerabilities, policy violations, and areas of particularly sensitive information that may be susceptible to attack or exposure. Our cloud experts will also compile for you a personalized and prioritized list of recommendations and suggested remediations that align your business objectives with regulatory compliance. Depending on how you choose to move forward, these same experts will then help you remediate the identified issues.

Once your environment is audit compliant, and/or all known issues have been addressed, the next phase is staying compliant. 2nd Watch's Managed Governance and Compliance solution is designed specifically to help you achieve on-going, continuous compliance. We monitor your environment for changes, alert our team of experts when suspicious or non-compliant activity is detected, work to identify and remediate the configuration drift causing the non-compliant state, and ensure that an up-to-date audit trail is kept at all times in compliance to applicable regulatory guidelines.

ASSESSMENT

- Thorough scanning of environment against industry standard compliance policies including PCI, HIPPA, GDPR, CIS, NIST, and SOC 2
- Vulnerability analysis with risk scoring
- Identification of suspicious network activity and exploitable hosts

REMEDIATION

- Audit trail investigation
- Resolution of resource misconfiguration
- Enforcement of change control policies

MAINTENANCE

- Real-time notification of policy violations with context to determine severity allowing prioritization when triaging issues
- Realtime asset inventory management
- Documentation of all platform management, incident response, and access management, as required to maintain compliance
- Ongoing assistance in creating and implementing new policies
- Log aggregation and retention

When it comes time for your regulatory audit, we will assist you in gathering the necessary documentation and reports your auditors request with Audit Assistance.

AUDIT ASSISTANCE

- Specific, point-in-time asset inventory
- Historic configuration change logs
- Assistance compiling information required for the audit

SERVICES	STANDARD	ADVANCED
Implementation of monitoring, auto-remediation, and reporting tools needed for continuous compliance	■	■
Training on how to utilize the compliance toolset	■	■
Ongoing monitoring of the compliance toolset	■	■
Industry-standard regulatory compliance evaluation and guidance (CIS, NIST, HIPAA, PCI-DSS, SOC2, GDPR)	■	■
Continuous compliance monitoring	■	■
Integration into workflow/ notification management systems[1]	■	■
Real-time notification of compliance policy violations	■	■
Live view of current compliance status	■	■
Real-time asset inventory	■	■
Real-time compliance reports	■	■
Vulnerability & threat assessment with risk scoring	■	■
Tier 1 support for compliance toolset	■	■
Personal Compliance Specialist (assigned)		■
Remediation of policy violations according to predefined processes		■
Custom policy creation		■
Log aggregation and retention assistance		■
OS patch management with reporting		■
Enforcement of change control policies		■
Password & key management policy enforcement		■
Non-compliance root cause analysis assistance		■
Up-to-date platform management procedures		■
Up-to-date incident response procedures		■
Up-to-date access management procedures		■
Up-to-date process flow documentation		■
Assistance in audit preparation (running reports, providing/locating documentation)		■
Quarterly compliance reviews with recommendations		■

[1]Limited to the workflow/notification's services supported within the compliance toolset including, AWS SQS, Splunk, email, Slack, and Jira.

1-888-317-7920
info@2ndwatch.com
www.2ndwatch.com