# SERVICE COMPLIANCE MONITORING

ActiveBytes compliance monitoring service helps you to introduce and maintain the compliance measures no matter the complexity. A simple misconfiguration or missed product update may not only harm the security of the network but may also expose the organization to compliance-breaching conditions. In such a situation, the investment already made in security systems becomes meaningless. Our team helps you to avoid such security breaches that can subject you to legal actions, financial impact and the negative impact it brings on customer trust.
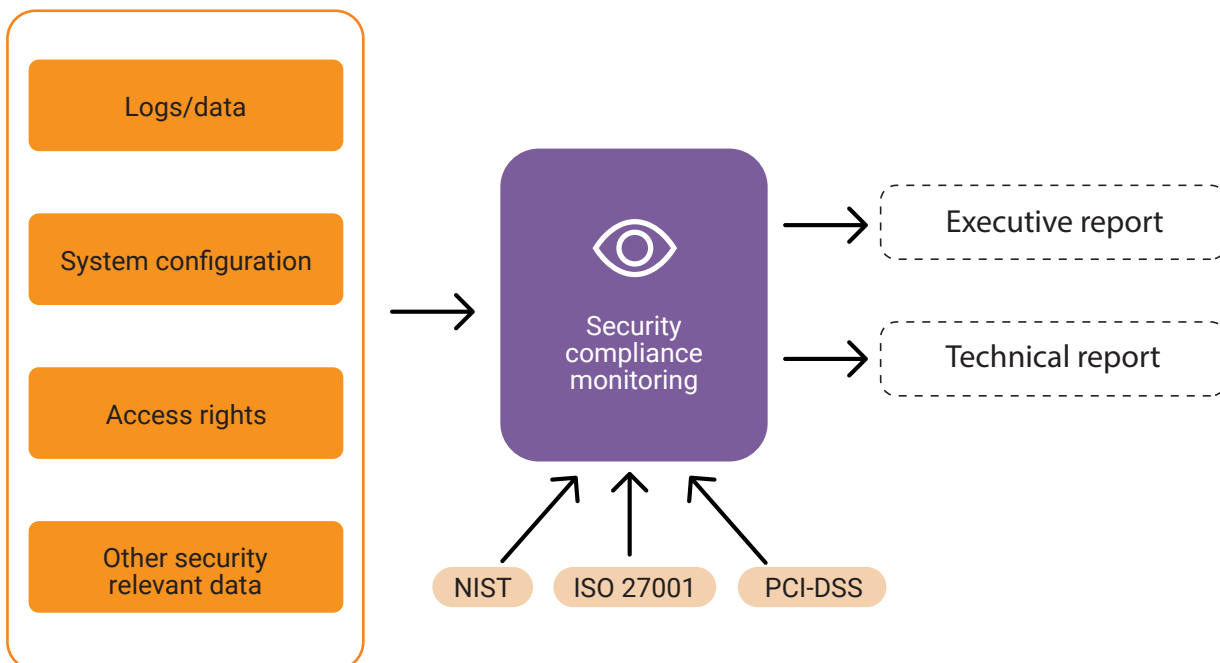
Every event log from the enterprise IT environment will be correlated against the regulatory controls as per the organization standards requirement. The potential deviations from the compliance will be documented, its impact including financial and legal issues will be detailed and cost-effective solutions for remediation will be reported.

Our approach

- Alignment of information security objectives with business objectives
- Risk-based implementation of security controls
- Individual approach
- Leveraging experience with many advanced security incidents during the implementation of security controls

Methodology

Identify all security requirements
Determine the scope of implementation
Assess existing security measures
Risk assessment
Create an implementation plan
Implementation of security measures and processes
Measurement, monitoring, review, and continuous improvement
Preparation for certification

Information security audit

Audit of the information security documentation

We examine the adequacy and effectiveness of information security documentation to identify gaps in information security management. It consists mainly of security strategies, policies, guidelines, procedures, manuals and operation of the information security system. We will also review asset management, risk management, information classification schemes, access control and any other security documentation.

Audit of processes

Our auditors examine how processes work and assess the extent to which internal and external requirements are met. During interviews with the staff responsible for these processes, the current state

![logo](activebytes innovations)

will be reviewed. Then, it will be assessed whether these processes are clearly defined, documented and whether all stakeholders know their role. As part of the final audit report, we will also provide recommendations for resolving the identified gaps.

Audit of compliance with a standard

We aim to examine the extent to which the requirements of security standards and legislation are met. The scope of the audit heavily depends on the standard of reference. As part of the compliance audit, our auditors examine internal policies, documented procedures, and various records demonstrating that the security system is operating as intended.

Technical security audit

Our team examines the security configurations of servers, endpoints, network and security devices. The hardening of equipment and the implementation of technical security measures are also examined. As part of audit activities, auditors focus on security logs, firewall rules, encryption, backup and other aspects of information security.

Benefits

- Simplified tracking of regulatory changes
- Fosters customer satisfaction & trust
- Reduce legal problems
- Drive strategic growth through resource focus
- Reduce risk through alerting on compliance violating events
- Internal or regulatory compliance policies auditing requirements fulfilled
- Holistic approach through event coverage across the enterprise