GRA QUANTUM

Managed Security Services & Compliance Readiness

Meeting regulatory compliance requirements can be a challenge for many businesses, especially start-ups, small-to-medium businesses (SMB), and those who cannot justify the expense of a full IT security department or compliance team. Below are the top compliance concerns and how GRA Quantum's services can help companies strategically align to standards such as HIPPA, PCI DSS, ISO 2700, and NIST.

Maintain Firewall Configuration

Based on an organization's business and type of data handled, this can require anything from regular auditing of firewall configurations, to change control for firewall rules and updates.

- Our MSSP can monitor for configuration changes, perform regular audits, and even fully manage your firewall solution.

System Passwords

Most regulatory compliance requirements contain controls to change system default passwords, enforce password complexity requirements, and regular password changes.

- Auditing and scanning of systems in scope for MSSP will be monitored for weak passwords, default or blank passwords, and can be configured to enforce these password requirements.

Sensitive Data Processing

Sensitive data such as Protected Health Information (PHI), Personally Identifiable Information (PII), and credit card data must be locatable, and encrypted in transit and at rest.

- If a customer has implemented software to locate and encrypt data, this can be monitored and verified by the MSSP. If this is a service the customer needs to implement, we can work to find an acceptable solution, whether it's managed or unmanaged.

Protect Endpoints

To meet compliance requirements, all endpoints must be protected with anti-virus or endpoint protection software. These must be updated regularly. File Integrity Monitoring on critical systems is also frequently a requirement.

- As part of the MSSP, endpoint protection is offered as a managed service or to be included in monitoring fees. We can implement and monitor File Integrity Monitoring solutions, as well as endpoint protection.

info@graquantum.com | 1(888) 610-6080

Secure Applications and Systems

Systems and Applications deployed in a compliance scoped environment must be secured and regularly patched.

- The GRAQ MSSP can perform vulnerability and configuration scanning on all systems to ensure these requirements are met.

Secure Data

Sensitive data must be secured on a "need to know" basis. This includes physical access to the data.

- The MSSP can perform regular audits of data access to ensure only those who need access have access.

Authentication

Most regulatory compliance requirements include sections about secure authentication. Many require that access to sensitive data requires strong authentication and even multi-factor authentication.

- The MSSP monitor critical systems and data, to ensure data is never stored or accessible in an area where authentication is not required.

Access is Monitored

Physical or logical access to sensitive data must always be logged and tracked.

- Our MSSP services always include logging support and monitoring of those logs.

Routine Security Testing

Compliance requirements usually require penetration and other security testing on at least an annual basis. Some compliance entities may require other security assessments.

- GRAQ has a wide range of consultants ready and able to perform penetration testing and security assessments.

Maintain Documentation

Security policies, incident response plans, and other documentation is not only required, but must be updated on a regular basis.

- GRAQ consultants can help to create, review, and maintain security related documentation to meet compliance requirements.