Information Security

OVERVIEW

Comprehensive review of existing disaster recovery architecture: reviews that highlight an institution's regulatory strengths and weaknesses.

Documented solution that assures compliance with the regulations, rules, and laws governing the safeguarding of personal information contained in both paper and electronic records.

The first and only full-service mortgage risk management firm in the country.

Lenders Compliance Group

866-602-6660

www.LendersComplianceGroup.com

Offices throughout the United States

INFORMATION SECURITY

CYBERSECURITY

RISK ASSESSMENT

POLICY AND PROCEDURES

Disaster Recovery

- Review the availability of ongoing systems, which includes the review of processes, policies, and controls used to ensure authorized users have prompt access to information. The objective it to protect against intentional or accidental attempts to deny legitimate users access to information or systems.
- Evaluate the integrity of data or systems, in order to ensure that the processes, policies, and controls used to ensure information have not been altered in an unauthorized manner and that systems are free from unauthorized manipulation that will compromise accuracy, completeness, and reliability.
- Determine the confidentiality of data or systems, which includes the processes, policies, and controls employed to protect information of customers and the institution against unauthorized access or use via Internet, Cyber, and Information Security protocol.
- Identify the institution's data, application and operating systems, technology, facilities, and personnel; and business activities and processes within each of those categories.
- Use a measurement or scoring system that ranks and evaluates business and control risks for significant business units, departments, and products.
- Review accountability and responsibilities set forth in processes, policies, and controls necessary to trace actions to their source. Accountability directly supports non-repudiation, deterrence, intrusion prevention, security monitoring, recovery, and legal admissibility of records.
- Evaluate technical and operations assurance levels, as further specified in processes, policies, and controls, in order to develop confidence that technical and operational security measures work as intended. Assurance levels are part of the system design and include availability, integrity, confidentiality, and accountability. Assurance highlights the notion that secure systems provide the intended functionality while preventing undesired actions.
- Review existing IT, IS, and Cyber policies and procedures and, where needed, either revise or replace them in order to ensure compliance with federal and state banking and consumer lending law.

FOR MORE INFORMATION

Kevin Origoni, Six Sigma

Director/IT, IS, and Cybersecurity

KOrigoni@LendersComplianceGroup.com

866-602-6660 x 104