InfoSight's IT General Controls Objectives

General IT Controls Review (GITCR) – InfoSight Overview

InfoSight's GITCR will go over your IT Control Policies and analyze the current condition of such policies to make necessary changes to ensure regulatory compliance. This review will also provide the foundation to assist the Institution in aligning its control environment with industry best practices. Overall, the review will serve as a tool for managing risk levels as the Institution moves forward with its future growth strategy. We separate our GITCR within different objectives to align with your company's goals, best practices and compliance.

IT Management Objectives

- Adequacy of IT governance and management activities
- Adequacy of IT planning and risk review
- Oversight over control processes – BCP, Information Security (GLBA compliance), outsourcing, development & acquisition and operations as needed
- Effective reporting and IT- risk monitoring
- Appropriateness of policies, procedures, and controls based on organizational complexity

BCP/DRP Objectives

- Interview management and review the business continuity request information to Identify changes to business, resources, technology, service providers, or any other impacting and relevant changes
- Determine whether an adequate BIA and risk review have been completed.
- Determine whether appropriate risk management over the business continuity process is in place.
- Determine the existence of an appropriate enterprise wide BCP
- Determine whether the BCP includes appropriate hardware back-up and recovery.
- Determine that the BCP includes appropriate security procedures.
- Determine whether the BCP effectively addresses pandemic issues.
- Determine whether the BCP addresses critical outsourced activities.
- Determine whether the BCP testing review is sufficient to demonstrate the financial institution's ability to meet its continuity objectives.
- Determine whether the appropriate level of Cyber-resiliency is considered within the BCP.

Information Security Objectives

- Determine the existence of new threats and vulnerabilities to the institution's information security.
- Determine the complexity of the institution's information security environment
- Quality of risk management (see Management section). Assure sufficient points are in the review
- Evaluate adequacy of security policies.
- Vendor security related controls - See outsourcing section
- Adequacy of security monitoring
- Enterprise wide security admin

Outsourcing Technologies Objectives

- Interview management and review institution information regarding sourcing practices
- Evaluate the quantity of risk present from the institution's outsourcing arrangements.
- Evaluate the outsourcing process for appropriateness, given the size and complexity of the institution.
- Evaluate the service provider selection process.
- Evaluate the process for entering into a contract with a service provider.
- Contracts contain the following relative to outsourcing engagements.
- Determine if the organization has a process to monitor that the vendor is fulfilling their obligations outlined within the contract (e.g. Service Level Agreements (SLAs), Knowledge Performance Indicators (KPIs)/Knowledge Risk Indicators (KRIs)).
- Evaluate the overall governance of the outsourcing review.
- Review policies regarding periodic ranking of service providers by risk. The decision process should:
- Evaluate the financial institution's use of user groups and other mechanisms to monitor and influence the service provider.