# Core Conversion Considerations

Core service providers supply a mission-critical function for financial institutions for centralized operations and data management, operational efficiency and automation, digital integration, security and compliance, and reliability. When a financial institution makes a strategic decision to convert to a new core service provider, fundamental considerations, plans, and execution are vital to ensure data integrity, accessibility, and functionality. Sound governance dictates that adequate planning, resources, and technical competence should be deployed during the states of planning, migration, and post-conversion. Thorough due diligence is paramount and needs to be supported with regular reporting and approval from the board of directors. Full consideration should be given to all aspects of the end-to-end process from inception.

## Core Conversion Project Planning

The process of core conversion should begin with a thorough project plan that acts as governance for the full conversion process. The project plan should identify current core system strengths, weaknesses, pain points, and limitations. Management should configure the new system so it addresses the financial institution's specific requirements. The newly considered core service provider should be evaluated based on this assessment, and the project plan should fully incorporate the financial institution's goals and outcomes for the new system. A project manager should be dedicated and lead a cross-functional conversion team with technical skills necessary to successfully oversee the conversion process. The team should develop and execute an effective communication plan to consider all stakeholders including employees, board members, customers, vendors, regulators, and any other impacted group.

A thorough evaluation and development of a realistic budget and financial impact analysis should be performed for the new core, ancillary systems, deconversion, and other support costs necessary with ongoing operations and sunsetting of systems to be replaced. Timing of sunsetting the existing platform and running on the new platform should be evaluated to ensure there will be no break in core provider services. A review of the fidelity bond coverage for system errors, interruption of service, errors, etc. should also be performed.

The vendor selection process should include a thorough due diligence of the new core system provider. Considerable attention should also be given to the vendor contract. Vendor contracts should receive professional legal review that include areas such as total cost of ownership, flexibility, functionality, service level agreements, , security and compliance, operability with other systems and functionality, termination of the relationship, etc. A thorough risk assessment should be performed for the project. The risk assessment should include the risk of untimely or failed system integrations and contain contingency plans to mitigate identified risks.

Reliable and accurate data is essential for successful conversion. Management should ensure that data is verified for data quality purposes prior to the conversion. Management should also identify all third-party integrations and file mapping in advance. This includes documenting current operational processes with the existing core system to align configurations. Consideration should also be given to access and ownership of the legacy core data.

Migration

Migration should be guided by a comprehensive data migration plan addressing mapping of all data into a standard format approved by the new vendor. This should include a determination that management has configured the new system to satisfy financial institution requirements. Formal testing plans should include appropriate end users, sufficient load testing, and a formal issue-tracking and resolution process.

Implementation of training plans, socialization and awareness campaigns, and educational materials should continue during this phase for both employees and customers. This includes communication steps to keep customers updated on the conversion progress and addressing questions. Considerations of customer information security, downtime, customer communications, and resolution of processing issues should be thoroughly considered through this stage. Sufficient staff support should be addressed and available for increased customer communication and vendor integration requirements.

Criteria should be defined to pre-determine go-live readiness. Contingency plans should be established if go-live is delayed, including continuation of critical business and/or critical operations without interruption.

Post Conversion

System validation is vitally important. Management should verify that data has been accurately transferred and the system is functioning as expected for data integrity and consistency. The verification should align with previously established performance and data quality requirements. Monitoring should be continuous after the system is initially implemented. Any unplanned operational issues should be continuously assessed until resolved.

Management should ensure appropriate system security settings are established. This should include reviewing and confirming remote connection access levels; ensuring integrity of default security settings and passwords for all core components; verifying core data-in-transit and data-at-rest is encrypted by default; establishing procedures to ensure core updates, security patches, and other updates are regularly applied; confirming security access level groups and administrators; verifying testing and production environments; and performing a penetration test and vulnerability assessment of the network.

Ongoing support and resources should continue for internal employees and external customers using the new system. An action plan to identify any issues, implement corrective action, track status, and monitor resolution timeframes should be executed. Management should complete a thorough “lessons learned” analysis at the end of the project to gain insights for future projects and create institutional knowledge. Impacted areas to evaluate include an assessment of the conversion causing any unexpected system downtime or any incorrect transactions or fees to post to customer accounts. Key issues should be reported to the core vendor for informational and assistance purposes.

Additional Resources

While the areas outlined above provide a general overview of key considerations before, during, and after core conversion, these areas should not be viewed as an exhaustive list of factors for the Board and management to evaluate. For additional resources for managing third-party relationships, the Board and management should review the *Interagency Guidance on Third-Party Relationships: Risk Management*, which provides sound principles that support a risk-based approach to third-party risk management. Furthermore, the Board and management should also review the FFIEC IT Handbook for additional information regarding core conversions and risk management practices.