Checklist to Define the Scope of Electronic Discovery

Due to the nature in which data is generated during the course of normal business operations, defining the scope and evaluating potential sources of electronic information relevant to a legal matter for electronic evidence is vital to ensure efficient, effective, and economical electronic discovery. To facilitate the collection, analysis, and preservation of electronic evidence, the following elements should be identified:

❑ The architecture and elements of the technology infrastructure, including, but not limited to, the amount and types of computers, operating systems, and software applications

❑ The topology of the network environment, including, but not limited to, the physical placement of computers and their connectivity within the intranet and Internet

❑ The formation of the electronic mail system, including, but not limited to, server and workstation software, lists of users, and location of email files

❑ Enterprise user information applications, including, but not limited to, contact lists, calendars, to do lists, word processing, project management, and accounting

❑ Internal and external personnel responsible for the management and maintenance of the technology infrastructure and all of its components

❑ Backup policies and procedures, including, but not limited to, hardware and software used to backup and archive information, documentation of what data is backed up, backup schedules, and locations of all backup media devices

❑ Computer use policies and procedures, including, but not limited to, employee guidelines, password utilization, system logging, security controls, data retention, information sharing, and acceptable Internet usage