Compliance Preparation Checklist

To start your business impact analysis, you must first complete an inventory of the systems in your IT environment. This requires understanding what functions they perform for the business, the parties that own and use the system as well as the individual components that the system is comprised of.

Configuration Information		
☐	Network Diagram	A visual representation of all devices that reside on the network including all connections to and from the network and details for each device installed
☐	Firewall Rules	A listing of all traffic explicitly allowed to and from each security zone including a justification for each permitted port/protocol
☐	System Build Documents	A detailed description of configuration parameters used to build each system including any quality assurance performed
☐	Data Encryption	A summary of technology deployed to ensure that data is encrypted both at rest and in transmission
☐	User Management	A listing of all active users within the system domain including permissions granted and justification

Policies & Procedures		
☐	Information Security Program	Including usage policies, training, service provider responsibilities, an information security manager and incident response for breach
☐	Responsibility Matrices	A listing of all roles within the organization and responsibilities as they pertain to each IT system
☐	Change Management	Including requirements for approval, testing following change implementation and backout contingencies
☐	User Management & Access Control	Including all physical and logical controls in place in order to obtain access to network, systems and data
☐	Key Management	Including key custodians, distribution, storage and retirement
☐	Password Standards	Including requirements for strong passwords, process for password changes and lost passwords
☐	Configuration Reviews	Including regular review and validation of system and security configuration
☐	Application Development	Best practices for developing applications and testing/deploying code updates
☐	Media Handling	Including security of media storage devices and destruction of data upon decommission
☐	Business Continuity	Including how to recover regular business and IT operations in the event of a disaster and documented regular testing of the plan

Logging & Sampling		
☐	Vulnerability Scanning Results	Documentation proving regular updates are performed and identified risks are remediated
☐	Penetration Testing Results	Documentation proving regular updates are performed and identified risks are remediated
☐	Operating System Patching	Documentation proving regular updates are performed and identified risks are remediated
☐	Anti-Virus	Documentation proving regular updates are performed and identified risks are remediated
☐	Intrusion Detection	Documentation proving regular updates are performed and identified risks are remediated
☐	Web Application Firewall	Documentation proving regular updates are performed and identified risks are remediated
☐	Logical Access	Documentation showing all access to systems
☐	File Modification	Documentation showing all modifications made to critical files
☐	Physical Access	Documentation showing all physical access to locations where data is stored