ESD IT Project Deliverable Criteria

In addition to a list of mandatory business requirements for any ESD contract or project with an IT component, the following deliverables should be evaluated for inclusion in the Statement of Work (SOW) and if necessary, be further clarified based on specific project requirements:

a. Mandatory Deliverable-Security Compliance
   - Partners, contractors, vendors, suppliers and all other 3rd parties working with ESD or ESD's contracted vendors must comply with ISO Standards 27001, 27005 and 27035 as they relate to the protection of ESD's network, data and information systems. For more information about these and other ISO standards visit https://www.iso.org
   - Must have monitoring process in place and documented for 3rd party compliance
   - Must provide documentation certifying that all 3rd party vendors in the supply chain are complying with ISO standards 27001, 27005 and 27035 as related to their role in the project
   - Must document all 3rd party access to ESD data or information systems
   - Must manage Information Communications to maintain the security of ESD data
b. Mandatory Deliverable – Security Management Plan
   - Data Security model, including classification, controls and encryption
   - Data Retention
   - Transaction Security including definition of user roles
   - Physical Security, including disaster recovery, continuity and backups
   - Identity Access Management, including authentication and transaction auditing
   - Patch Management approach
   - Security Logging
   - Vulnerability Scanning, monitoring and remediation
   - Adherence to NYS and Federal Cyber Security and Information Security Polices and Laws
c. Deliverable – Project Approach
   - Deliverables Approach
   - Criteria for Deliverable Acceptance
   - Technical Approach
   - Issue Management
   - Risk Management
   - Secure System Development Life Cycle
   - Quality Assurance Approach
   - Communications Approach (Project Kickoff, Status Reporting, etc.)
   - Project Schedule
d. Deliverable – Business Requirements Validation
   - Refinement of mandatory requirements
e. Deliverable – Infrastructure Build & Configuration
   - Hosting Model (on / off premise)
   - Servers
   - Software
   - Hardware
   - Security
f. Deliverable – Technical Environments
   - Development / Test
   - Staging
   - Production
g. Deliverable – Interface Requirements

- Does the system need to interface with other ESD or 3rd party Systems?
- Interface Design
- Data Migration

h. Deliverable – Testing
   - Define testing criteria and approach

i. Deliverable – Training
   - Training Plan
   - Training Materials

j. Deliverable – Service Level Agreement (SLA)
   - SLA levels provided
   - Monthly reporting of SLA activities
   - Penalties for not meeting SLA criteria

k. Deliverable – Support
   - Define support levels and responsibility

l. Deliverable – Implemented System
   - Fully functional production system

m. Deliverable – End of Contract Transition
   - Documentation outlining procedures and timelines for returning all ESD owned systems, software, equipment, licenses, data and intellectual property back to ESD
   - Agreed upon data format for returned information
   - Policy for final purging of ESD data from 3rd party systems, backups and disaster recovery sites