

## **Enterprise Systems Management (ESM) Best Practices:**

- Best Practice 1.** Agencies should establish an Incident Management process and procedures; the process and procedures shall enable restoration of normal service operation as quickly as possible and minimize the impact on business operations.
- Best Practice 2.** Agencies should establish a system event monitoring console and institute systems performance alert thresholds ensure systems faults are averted and corrective measures are taken to limit the chance of total systems failure.
- Best Practice 3.** Agencies should utilize a Service Desk facility that is staffed with properly trained personnel who can minimally respond to level 1- type problems, incidents, and events. The Service Desk shall utilize an automated contact management tool and is the single point of contact for all IT service requests and services communications.
- Best Practice 4.** Agencies should establish an IT disaster recovery plan. This risk-based plan shall incorporate the operating constraints of the business continuity plan. In addition, there shall be procedures to test the IT disaster recovery plan periodically and update the plan.
- Best Practice 5.** Agencies with ESM responsibilities should institute procedures for problem handling. These procedures shall include steps for performing root cause analysis of incidents and correction of the error to the satisfaction of the customer.
- Best Practice 6.** Agencies should establish a release management process. Process activities shall include procedures for hardware, license/version control across the infrastructure, rollout planning, communication protocols, and quality control of the process.
- Best Practice 7.** Agencies should ensure critical back-up data files are rotated to an Off-Site location on a scheduled basis as defined in the back-up and recovery procedures. In addition, Off-Site locations shall comply with data security requirements such as encryption; as defined in the security domain.
- Best Practice 8.** ESM systems should be implemented in adherence with all security, confidentiality and privacy policies and applicable statutes.