Develop Contingency Planning Policy	Conduct Business Impact Analysis	Identify Preventive Controls	Create Contingency Strategies	Develop Contingency Plan*	Plan Testing, Training, and Exercises	Plan Maintenance
• Identify statutory or regulatory requirements • Develop IT contingency planning policy statement • Reflect FIPS 199 • Publish policy	• Determine business processes and recovery criticality • Identify outage impacts and estimated downtime • Identify resource requirements • Identify recovery priorities for system	• Identify controls • Implement controls • Maintain controls	• Backup & recovery • Consider FIPS 199 • Identify roles & responsibilities • Address alternate site • Identify equipment and cost considerations • Integrate into system architecture	• Document recovery strategy	• Plan testing • Train personnel • Plan exercises • TT&E activities	• Review and update plan • Coordinate with internal external organizations • Control distri-bution • Document changes

Source: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf

INGALLS
INFORMATION SECURITY

Cyber Innovation Center (CIC)
6300 Texas Street, Ste. 240, Bossier City, LA 71111
WWW.IINFOSEC.COM
(888) 860-0452