Recovery Preparation List

The following is a list of items that you will need to gather as part of your preparation for recovery.

1. **[Assets]** Inventory all the assets - servers, workstations, laptops, mobile devices, data (sensitive, confidential, corporate/client), on-prem/cloud, networking equipment, miscellaneous
2. **[Backups]** Inventory what is being backed up - record all of the assets being backed up, include the date backups where verified, the date recovery was tested on that asset group, if something is not being backed up, include a reason why, and the name of the technician who did these checks, and the manager who signed off on each line item. Include the name of the backup software being used and the backup strategy, backup schedule, backup retention, backup locations.
3. **[Configurations]** Inventory configuration files - these are backups of the network configurations, and other configuration files that can help recover the good configuration of a device or service quickly. (Cisco routers/switches, WIFI, software services configurations)
4. **[Diagrams]** Inventory the architecture diagrams (on-prem and cloud infrastructure / system design), network diagrams (subnets, VLAN, ports, protocols), data and backup architecture, security documentation (security tooling and security architecture decisions, GPO's, security policies, compliance frameworks)
5. **[Compliance]** Inventory the compliance and regulation requirements and reports - include any documentation that is relevant to maintaining compliance with each required privacy regulation
6. **[Contacts]** Inventory of staff, management and executives including contact information - at a minimum the department leads and managers for a larger organization so each department can be reached. Include personal phone number / email address, corporate email address so staff can be reached outside of regular work hours for emergencies.
7. **[Store the Inventory]** Cloud or offline storage of the inventoried documents and information so they are readily accessible during a severe cyber incident
8. **[Secure Communication Checklist]** Secure communications procedure and checklist