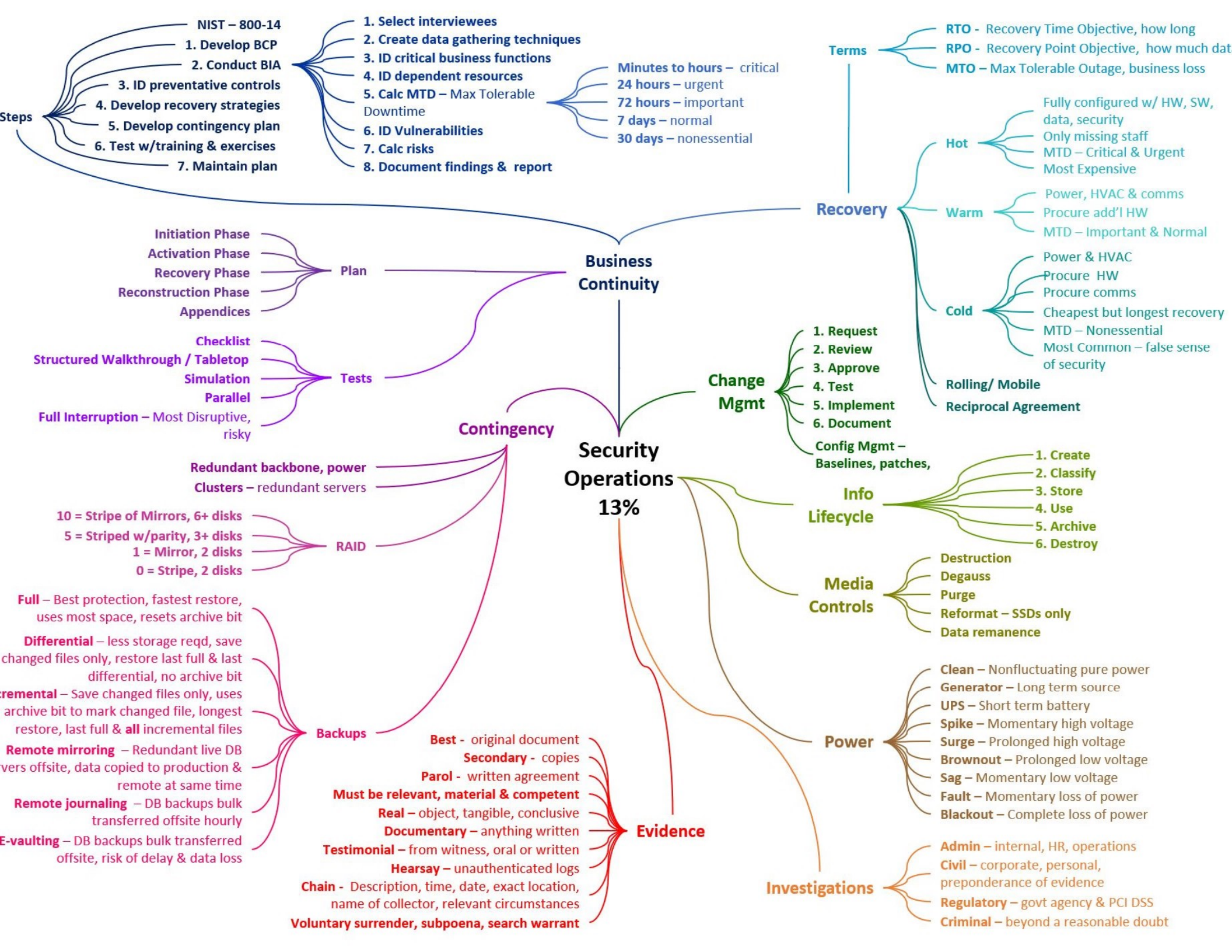
Steps
NIST – 800-14
1. Develop BCP
2. Conduct BIA
3. ID preventative controls
4. Develop recovery strategies
5. Develop contingency plan
6. Test w/training & exercises
7. Maintain plan
1. Select interviewees
2. Create data gathering techniques
3. ID critical business functions
4. ID dependent resources
5. Calc MTD – Max Tolerable Downtime
6. ID Vulnerabilities
7. Calc risks
8. Document findings & report
Minutes to hours – critical
24 hours – urgent
72 hours – important
7 days – normal
30 days – nonessential
Terms
RTO - Recovery Time Objective, how long
RPO - Recovery Point Objective, how much dat
MTO – Max Tolerable Outage, business loss
Recovery
Hot
Fully configured w/ HW, SW, data, security
Only missing staff
MTD – Critical & Urgent
Most Expensive
Warm
Power, HVAC & comms
Procure add'l HW
MTD – Important & Normal
Cold
Power & HVAC
Procure HW
Procure comms
Cheapest but longest recovery
MTD – Nonessential
Most Common – false sense of security
Rolling/ Mobile
Reciprocal Agreement
Business Continuity
Plan
Initiation Phase
Activation Phase
Recovery Phase
Reconstruction Phase
Appendices
Tests
Checklist
Structured Walkthrough / Tabletop
Simulation
Parallel
Full Interruption – Most Disruptive, risky
Change Mgmt
1. Request
2. Review
3. Approve
4. Test
5. Implement
6. Document
Config Mgmt – Baselines, patches,
Contingency
Redundant backbone, power
Clusters – redundant servers
RAID
10 = Stripe of Mirrors, 6+ disks
5 = Striped w/parity, 3+ disks
1 = Mirror, 2 disks
0 = Stripe, 2 disks
Backups
Full – Best protection, fastest restore, uses most space, resets archive bit
Differential – less storage reqd, save changed files only, restore last full & last differential, no archive bit
cremental – Save changed files only, uses archive bit to mark changed file, longest restore, last full & all incremental files
Remote mirroring – Redundant live DB vers offsite, data copied to production & remote at same time
Remote journaling – DB backups bulk transferred offsite hourly
E-vaulting – DB backups bulk transferred offsite, risk of delay & data loss
Security Operations 13%
Info Lifecycle
1. Create
2. Classify
3. Store
4. Use
5. Archive
6. Destroy
Media Controls
Destruction
Degauss
Purge
Reformat – SSDs only
Data remanence
Power
Clean – Nonfluctuating pure power
Generator – Long term source
UPS – Short term battery
Spike – Momentary high voltage
Surge – Prolonged high voltage
Brownout – Prolonged low voltage
Sag – Momentary low voltage
Fault – Momentary loss of power
Blackout – Complete loss of power
Evidence
Best - original document
Secondary - copies
Parol - written agreement
Must be relevant, material & competent
Real – object, tangible, conclusive
Documentary – anything written
Testimonial – from witness, oral or written
Hearsay – unauthenticated logs
Chain - Description, time, date, exact location, name of collector, relevant circumstances
Voluntary surrender, subpoena, search warrant
Investigations
Admin – internal, HR, operations
Civil – corporate, personal, preponderance of evidence
Regulatory – govt agency & PCI DSS
Criminal – beyond a reasonable doubt