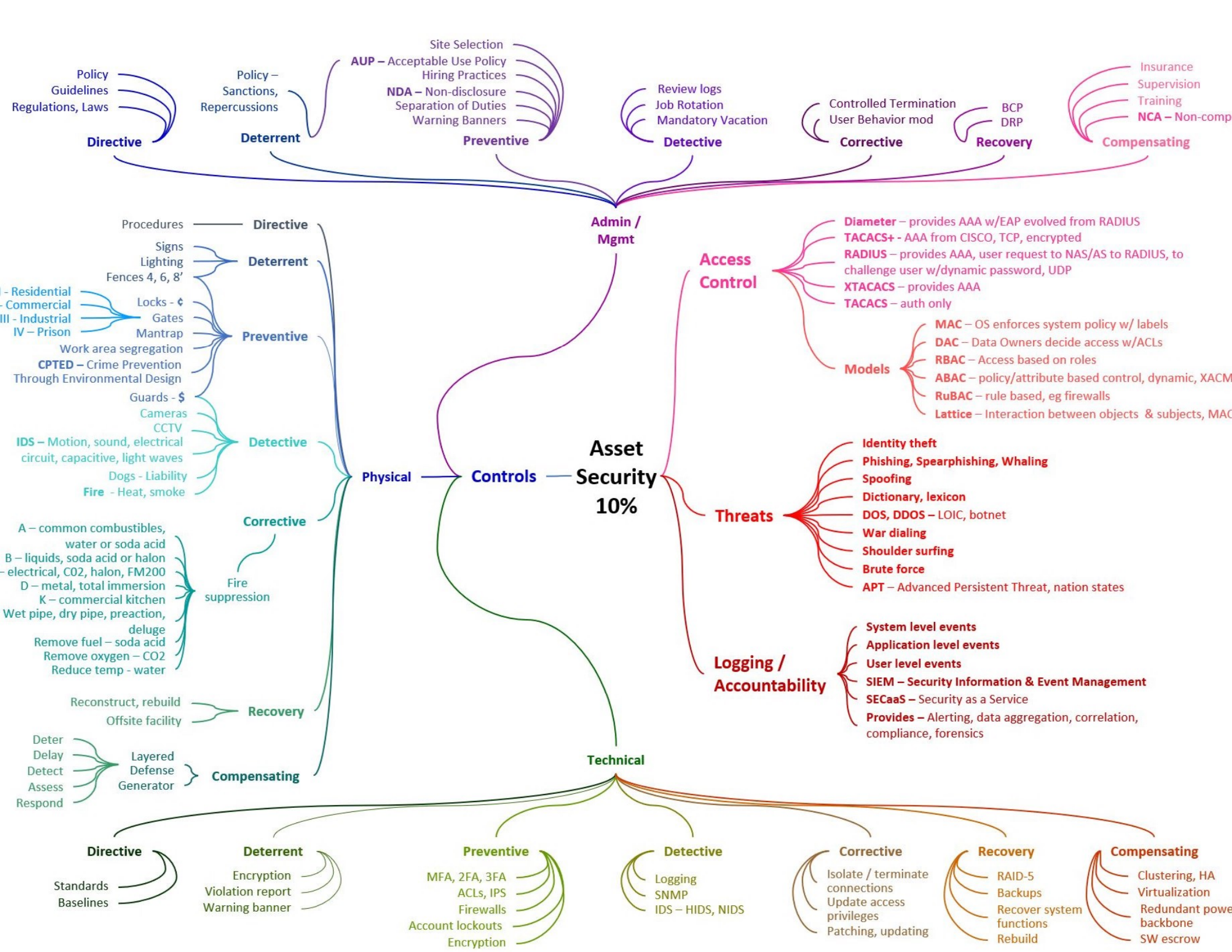
Asset Security 10%
Controls
Admin / Mgmt
Directive
Policy
Guidelines
Regulations, Laws
Deterrent
Policy – Sanctions, Repercussions
Preventive
Site Selection
AUP – Acceptable Use Policy
Hiring Practices
NDA – Non-disclosure
Separation of Duties
Warning Banners
Detective
Review logs
Job Rotation
Mandatory Vacation
Corrective
Controlled Termination
User Behavior mod
Recovery
BCP
DRP
Compensating
Insurance
Supervision
Training
NCA – Non-comp
Physical
Directive
Procedures
Deterrent
Signs
Lighting
Fences 4, 6, 8'
Preventive
Locks - ¢
Gates
Mantrap
Work area segregation
CPTED – Crime Prevention Through Environmental Design
I - Residential
II - Commercial
III - Industrial
IV – Prison
Detective
Guards - $
Cameras
CCTV
IDS – Motion, sound, electrical circuit, capacitive, light waves
Dogs - Liability
Fire - Heat, smoke
Corrective
Fire suppression
A – common combustibles, water or soda acid
B – liquids, soda acid or halon
C – electrical, C02, halon, FM200
D – metal, total immersion
K – commercial kitchen
Wet pipe, dry pipe, preaction, deluge
Remove fuel – soda acid
Remove oxygen – CO2
Reduce temp - water
Recovery
Reconstruct, rebuild
Offsite facility
Compensating
Layered Defense Generator
Deter
Delay
Detect
Assess
Respond
Technical
Access Control
Diameter – provides AAA w/EAP evolved from RADIUS
TACACS+ - AAA from CISCO, TCP, encrypted
RADIUS – provides AAA, user request to NAS/AS to RADIUS, to challenge user w/dynamic password, UDP
XTACACS – provides AAA
TACACS – auth only
Models
MAC – OS enforces system policy w/ labels
DAC – Data Owners decide access w/ACLs
RBAC – Access based on roles
ABAC – policy/attribute based control, dynamic, XACM
RuBAC – rule based, eg firewalls
Lattice – Interaction between objects & subjects, MAC
Threats
Identity theft
Phishing, Spearphishing, Whaling
Spoofing
Dictionary, lexicon
DOS, DDOS – LOIC, botnet
War dialing
Shoulder surfing
Brute force
APT – Advanced Persistent Threat, nation states
Logging / Accountability
System level events
Application level events
User level events
SIEM – Security Information & Event Management
SECaaS – Security as a Service
Provides – Alerting, data aggregation, correlation, compliance, forensics
Directive
Standards
Baselines
Deterrent
Encryption
Violation report
Warning banner
Preventive
MFA, 2FA, 3FA
ACLs, IPS
Firewalls
Account lockouts
Encryption
Detective
Logging
SNMP
IDS – HIDS, NIDS
Corrective
Isolate / terminate connections
Update access privileges
Patching, updating
Recovery
RAID-5
Backups
Recover system functions
Rebuild
Compensating
Clustering, HA
Virtualization
Redundant powe backbone
SW escrow