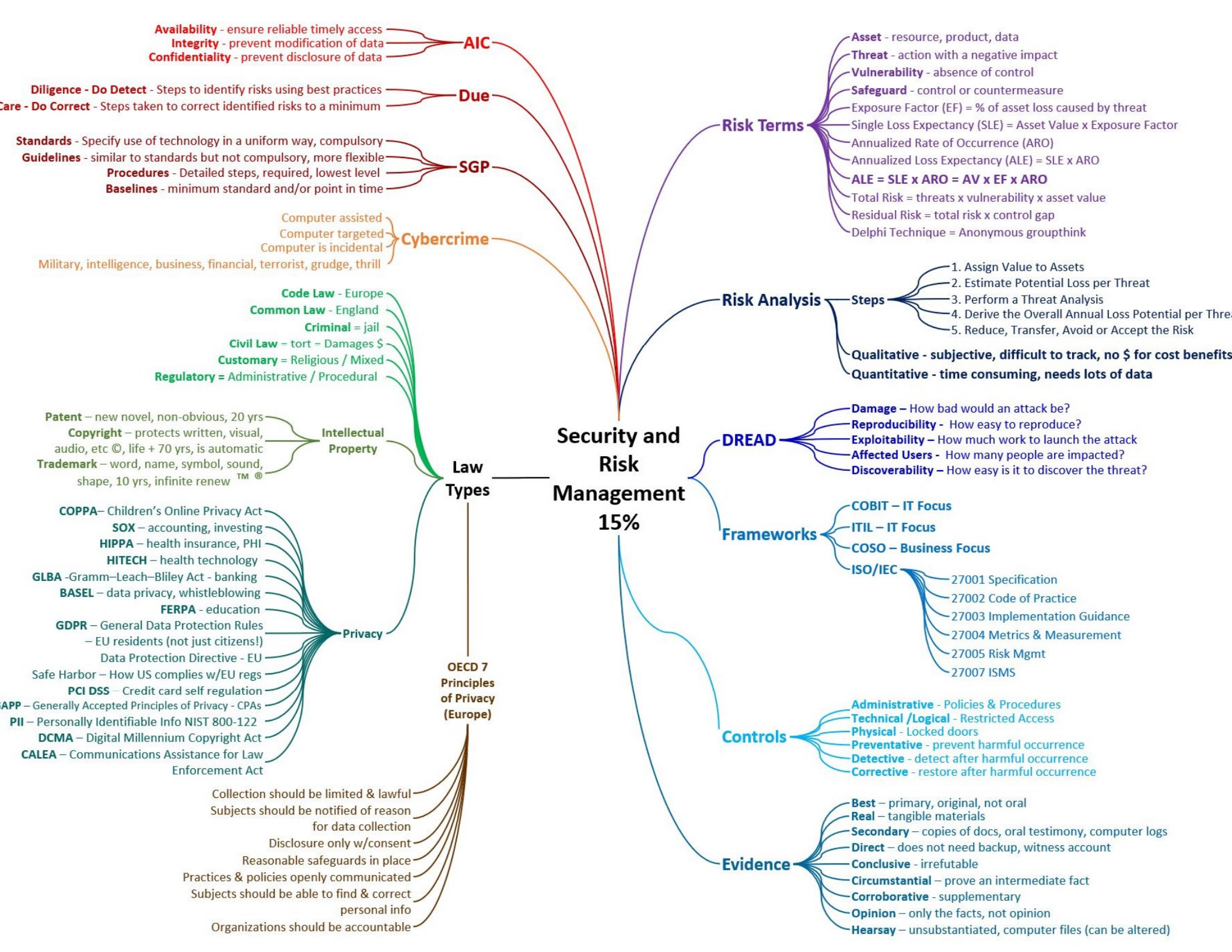
Security and Risk Management 15%
AIC
Availability - ensure reliable timely access
Integrity - prevent modification of data
Confidentiality - prevent disclosure of data
Due
Diligence - Do Detect - Steps to identify risks using best practices
Care - Do Correct - Steps taken to correct identified risks to a minimum
SGP
Standards - Specify use of technology in a uniform way, compulsory
Guidelines - similar to standards but not compulsory, more flexible
Procedures - Detailed steps, required, lowest level
Baselines - minimum standard and/or point in time
Cybercrime
Computer assisted
Computer targeted
Computer is incidental
Military, intelligence, business, financial, terrorist, grudge, thrill
Law Types
Code Law - Europe
Common Law - England
Criminal = jail
Civil Law = tort = Damages $
Customary = Religious / Mixed
Regulatory = Administrative / Procedural
Intellectual Property
Patent – new novel, non-obvious, 20 yrs
Copyright – protects written, visual, audio, etc ©, life + 70 yrs, is automatic
Trademark – word, name, symbol, sound, shape, 10 yrs, infinite renew ™ ®
Privacy
COPPA– Children's Online Privacy Act
SOX – accounting, investing
HIPPA – health insurance, PHI
HITECH – health technology
GLBA -Gramm–Leach–Bliley Act - banking
BASEL – data privacy, whistleblowing
FERPA - education
GDPR – General Data Protection Rules – EU residents (not just citizens!)
Data Protection Directive - EU
Safe Harbor – How US complies w/EU regs
PCI DSS – Credit card self regulation
GAPP – Generally Accepted Principles of Privacy - CPAs
PII – Personally Identifiable Info NIST 800-122
DCMA – Digital Millennium Copyright Act
CALEA – Communications Assistance for Law Enforcement Act
OECD 7 Principles of Privacy (Europe)
Collection should be limited & lawful
Subjects should be notified of reason for data collection
Disclosure only w/consent
Reasonable safeguards in place
Practices & policies openly communicated
Subjects should be able to find & correct personal info
Organizations should be accountable
Risk Terms
Asset - resource, product, data
Threat - action with a negative impact
Vulnerability - absence of control
Safeguard - control or countermeasure
Exposure Factor (EF) = % of asset loss caused by threat
Single Loss Expectancy (SLE) = Asset Value x Exposure Factor
Annualized Rate of Occurrence (ARO)
Annualized Loss Expectancy (ALE) = SLE x ARO
ALE = SLE x ARO = AV x EF x ARO
Total Risk = threats x vulnerability x asset value
Residual Risk = total risk x control gap
Delphi Technique = Anonymous groupthink
Risk Analysis
Steps
1. Assign Value to Assets
2. Estimate Potential Loss per Threat
3. Perform a Threat Analysis
4. Derive the Overall Annual Loss Potential per Threa
5. Reduce, Transfer, Avoid or Accept the Risk
Qualitative - subjective, difficult to track, no $ for cost benefits
Quantitative - time consuming, needs lots of data
DREAD
Damage – How bad would an attack be?
Reproducibility - How easy to reproduce?
Exploitability – How much work to launch the attack
Affected Users - How many people are impacted?
Discoverability – How easy is it to discover the threat?
Frameworks
COBIT – IT Focus
ITIL – IT Focus
COSO – Business Focus
ISO/IEC
27001 Specification
27002 Code of Practice
27003 Implementation Guidance
27004 Metrics & Measurement
27005 Risk Mgmt
27007 ISMS
Controls
Administrative - Policies & Procedures
Technical /Logical - Restricted Access
Physical - Locked doors
Preventative - prevent harmful occurrence
Detective - detect after harmful occurrence
Corrective - restore after harmful occurrence
Evidence
Best – primary, original, not oral
Real – tangible materials
Secondary – copies of docs, oral testimony, computer logs
Direct – does not need backup, witness account
Conclusive - irrefutable
Circumstantial – prove an intermediate fact
Corroborative - supplementary
Opinion – only the facts, not opinion
Hearsay – unsubstantiated, computer files (can be altered)