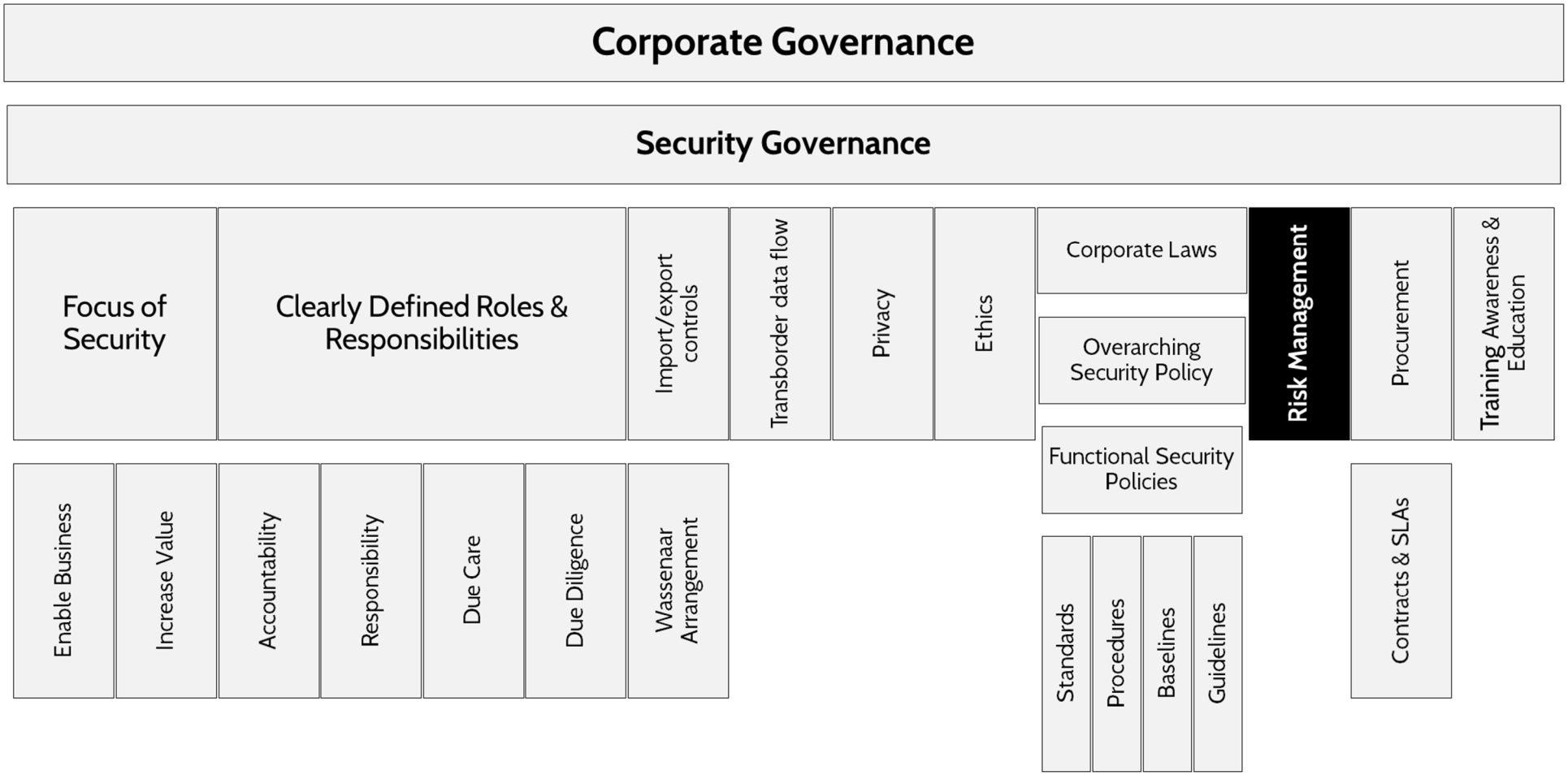
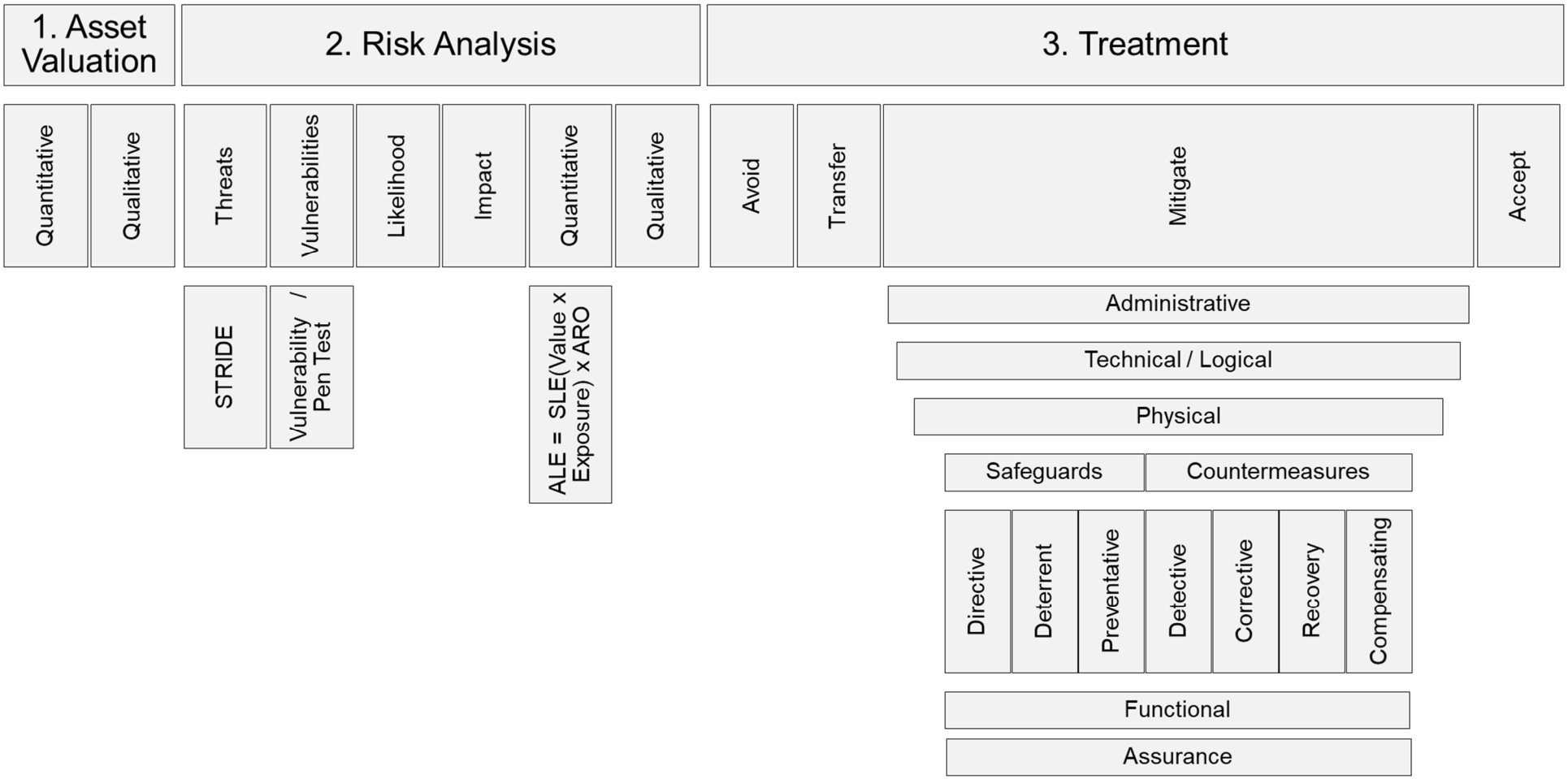
Alignment of Security Function to Business Strategy



© 2019 Destination Certification Inc.

Risk Management



© 2019 Destination Certification Inc.

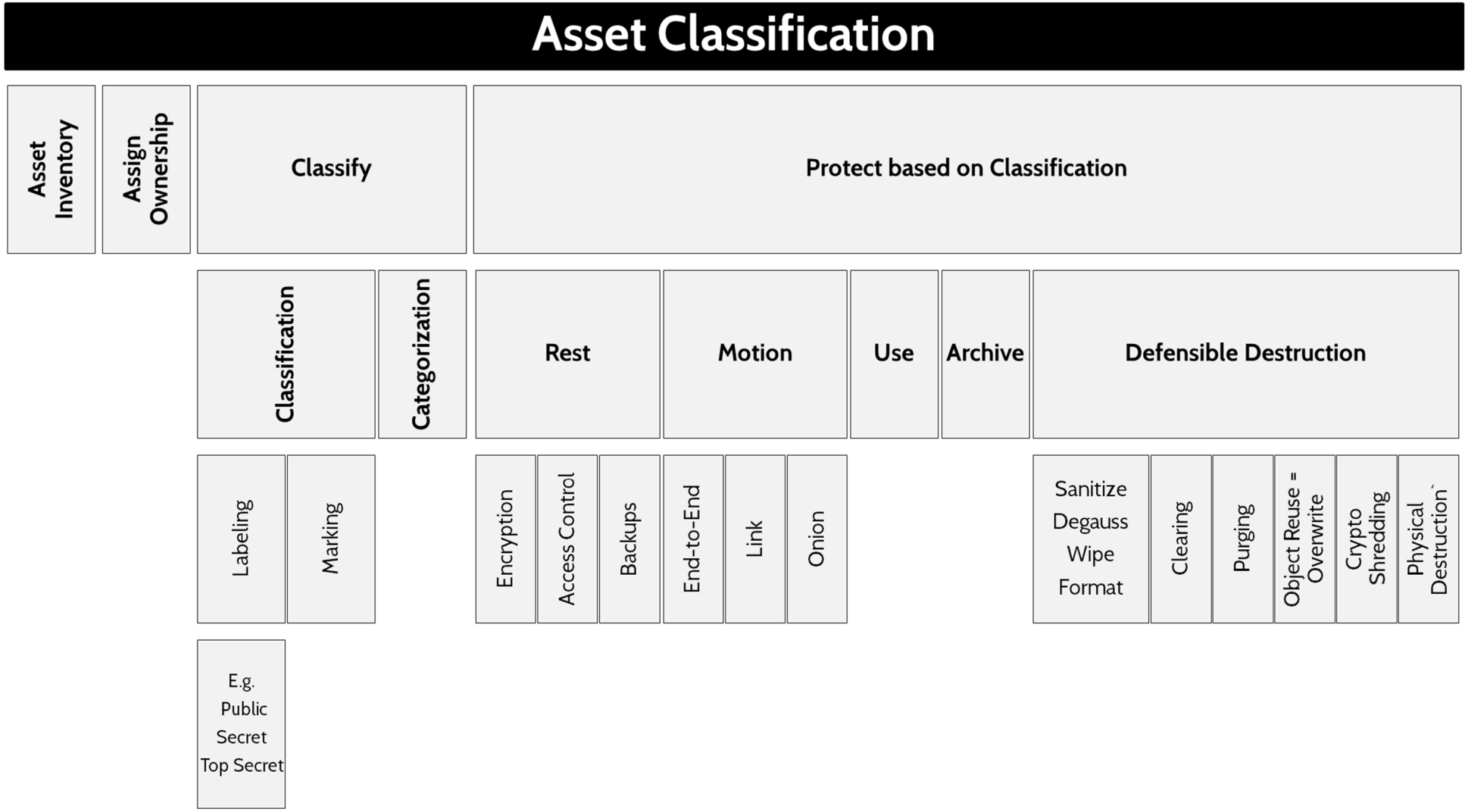
Intellectual Property

- Trade Secrets
- Patent
- Copyright
- Trademarks

Business Continuity Management (BCM)

- Business Impact Assessment
- Measurements of Time
  - RPO
  - RTO
  - WRT
  - MTD
- Types of Plans
  - Business Continuity Plan (BCP)
  - Disaster Recovery Plan (DRP)

© 2019 Destination Certification Inc.



© 2019 Destination Certification Inc.

Privacy

PII

- Direct Identifiers
- Indirect Identifiers

OECD Guidelines

- Collection Limitation
- Data Quality
- Purpose Specification
- Use Limitation
- Security Safeguards
- Openness
- Individual Participation
- Accountability

Roles

- Data Owner
- Data Custodian
- Data Steward
- Data Processor

© 2019 Destination Certification Inc.

Frameworks

Security							Privacy	Risk			
ISO 27001	NIST	COBIT	COSO	ITIL	HIPPA	SOX	OECD Guidelines	NIST 800-37	ISO 31000	COSO	ISACA Risk IT

Models

Enterprise Security Architecture			Security Models						
Zachman	Sabsa	TOGAF	Lattice Based			Rule Based			
			Bell-LaPadula	**Biba**	Lipner Implementation	Clark-Wilson	Brewer-Nash	Graham–Denning & Harrison–Ruzzo–Ullman	

© 2019 Destination Certification Inc.

Evaluation Criteria

Certification			Accreditation
TCSEC (Orange Book)	**ITSEC**	**Common Criteria**	
Functional Levels: D1, C1, C2, B1, B2, B3, A1	Functional Level + Assurance Levels: E0 - E6	EAL1 – EAL7	

© 2019 Destination Certification Inc.

Trusted Computing Base (TCB)

- Reference Monitor Concept
  - Subject
  - Mediation
    - Rules
    - Logging & Monitoring
  - Object
- Hardware Components
  - Processor
    - Multi-tasking
    - Multi-threading
  - Storage
    - Primary
    - Secondary
    - Virtual Memory
- Software Components
  - System Kernel
    - User Mode
    - Kernel Mode
  - Firmware
  - Middleware
- Protection Mechanisms
  - Process Isolation
    - Memory Segmentation
    - Time Division Multiplexing
  - Processor States
    - Problem
    - Supervisor
  - Secure Memory Management
  - Data Hiding
  - Virtualization / Abstraction
  - Defense in depth

- Security Kernel
  - Completeness
  - Isolation
  - Verifiability

© 2019 Destination Certification Inc.

Vulnerabilities in Systems

Single Point of Failure	**Bypass Controls**	**TOCTOU** (Race Conditions)	**Emanations**		**Covert Channels**	**Inference Aggregation**
Redundancy	Mitigating Controls	Increase Frequency of Re-authentication	Shielding (TEMPEST)	White Noise	Control Zones	Polyinstantiation

Web-based Vulnerabilities

Cross Site Scripting (XSS)			**Cross Site Request Forgery (CSRF)**	**SQL Injection**
Stored (Persistent)	**Reflected**	**DOM**		
Input Validation				

© 2019 Destination Certification Inc.

Cloud Computing

Characteristics					Service Models			Deployment Models			
On-Demand Self Service	Broad Network Access	Resource Pooling	Rapid Elasticity	Measured Service	IaaS	PaaS	SaaS	Public	Private	Community	Hybrid

© 2019 Destination Certification Inc.

Cryptographic Services

Confidentiality	Integrity	Authenticity	Non-Repudiation		Access Control
	= Hashing		Origin	Delivery	

Secret Writing

Hidden		Scrambled (Cryptography)								
Steganography	Null Cipher	One-way	Two-way						Substitution	Transposition
		Hashing	Symmetric			Asymmetric				
		MD5 SHA-1 SHA-3	Block		Stream	Factoring	Discrete Log		Caesar Cypher Monoalphabetic Polyalphabetic Running **One-time Pads**	Spartan Skytale Rail Fence (zigzag)
			DES **3DES** **AES** CAST-128 SAFER Blowfish Twofish RC5/RC6	**Block Modes:** **ECB** **CBC** **CFB** **OFB** **CTR**	RC4	RSA	Diffie-Hellmann Elliptic Curve (ECC) El Gamal DSS			

© 2019 Destination Certification Inc.

Digital Signatures

- Integrity
- Authenticity
- Non-repudiation

Digital Certificates

- Verify the owner of a Public Key
  - X.509
  - Replacement
  - Revocation

PKI

- Certificate Authority (Root of Trust)
- Registration Authority
- Intermediate CA
- Certificate DB (Revocation List)
- Certificate Store (Local)

Key Management

- Kirchhoff's Law
- Generation
- Distribution
  - Out-of-band
  - Hybrid
  - Key Wrapping
- Storage
  - TPM
  - HSM
- Rotation
- Disposition
  - Crypto-shredding
  - Key Destruction
- Recovery
  - Split Knowledge
  - Dual Control
  - Key Escrow

© 2019 Destination Certification Inc.

Cryptanalysis

Cryptanalytic Attacks

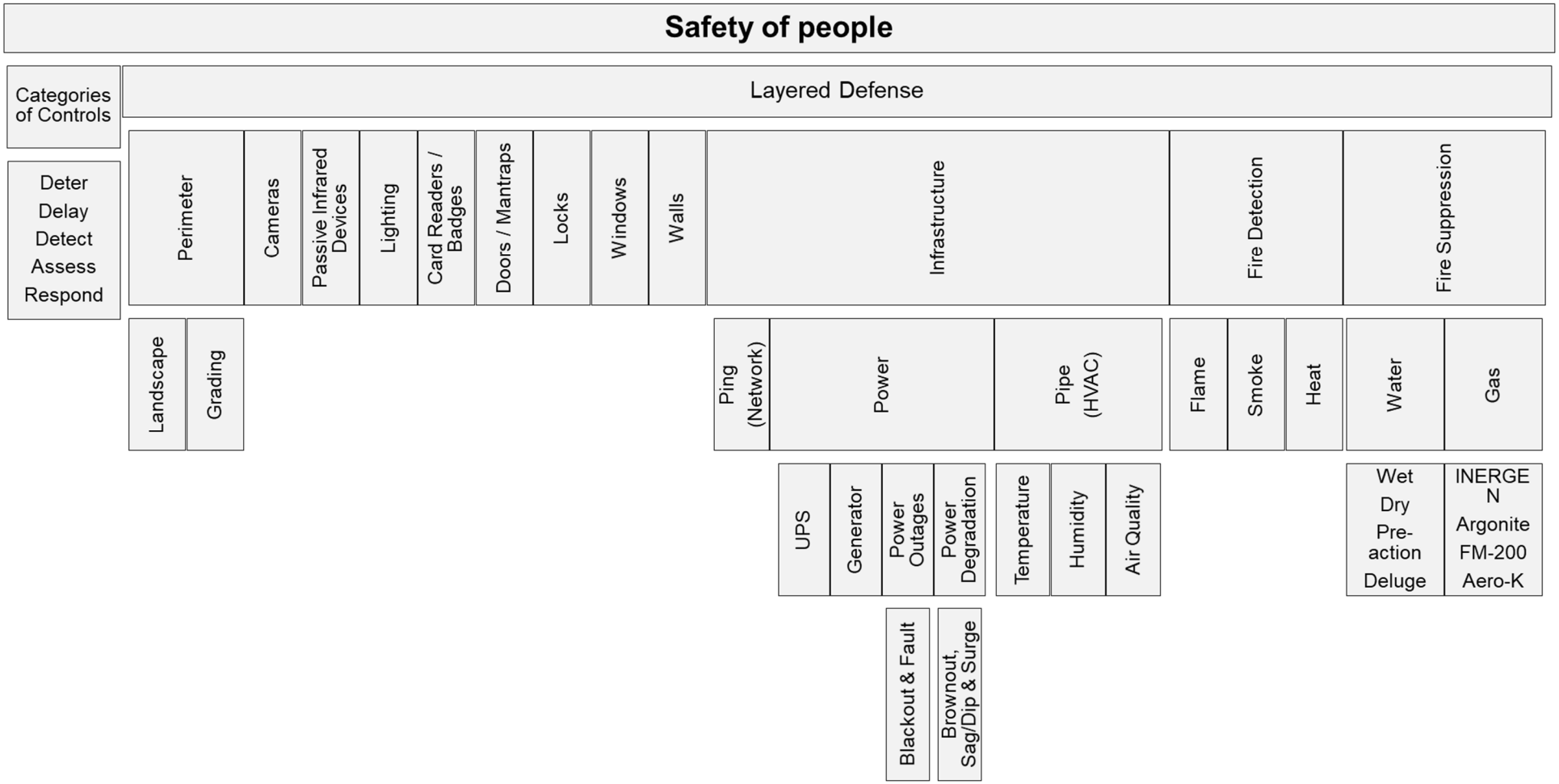
- Brute Force
- Ciphertext Only
- Known Plaintext
- Chosen Plaintext
- Chosen Ciphertext
- Linear & Differential
- Factoring

Cryptographic Attacks

- Man-in-the-middle
- Replay
- Temporary Files
- Implement-ation
- Side Channel
  - Power
  - Timing
- Dictionary Attack
- Rainbow Tables
- Birthday Attack
- Social Engineering
  - Purchase Key
  - Rubber Hose

© 2019 Destination Certification Inc.

Physical Security



© 2019 Destination Certification Inc.

Open Systems Interconnection (OSI) Model

7. Appl.	6. Presentation	5. Session	4. Transport	3. Network	2. Datalink	1. Physical
Devices		Devices	**Ports** = Services	**IP Address**	**MAC Address**	Media
Protocols		Protocols	Protocols	Devices	Circuit vs. Packet Switched Networks	Topologies
Application Firewalls		Circuit Proxy Firewall	**TCP/UDP & SSL/TLS**	**IPv4 & IPv6**	Devices	Collisions
HTTP/S, DNS, SSH, SNMP		PAP, CHAP, EAP		**Routers & Packet Filtering Firewalls**	Protocols	Devices
				ICMP (Ping), **IPSec,** IGMP	**Switches** & Bridges	**Wired:** Twisted Pair, Coaxial, Fiber Optic
					ARP, PPTP, SLIP, PPP, PAP, CHAP, EAP, PEAP	**Wireless:** Radio Frequency, Infrared, Microwave
						Bus
						Tree
						Star
						Mesh
						Ring
						CSMA/**CA**
						CSMA/**CD**
						Hubs, Repeaters, Concentrators

© 2019 Destination Certification Inc.

Networking

Converged Protocols	Network Attacks	Virtualization	WAN	Common Commands
iSCSI, FCoE, VOIP	Phases	VLAN	X.25	ipconfig
	Eavesdropping	SDN	Frame Relay	ping
	SYN Flooding		ATM	traceroute
	IP Spoofing		MPLS	whois
	Smurf / Fraggle			dig
	DoS / DDoS			
	Man-in-the-Middle			
	Spoofing			
	ARP poisoning			

Reconnaissance
Enumeration
Vulnerability Analysis
Exploitation

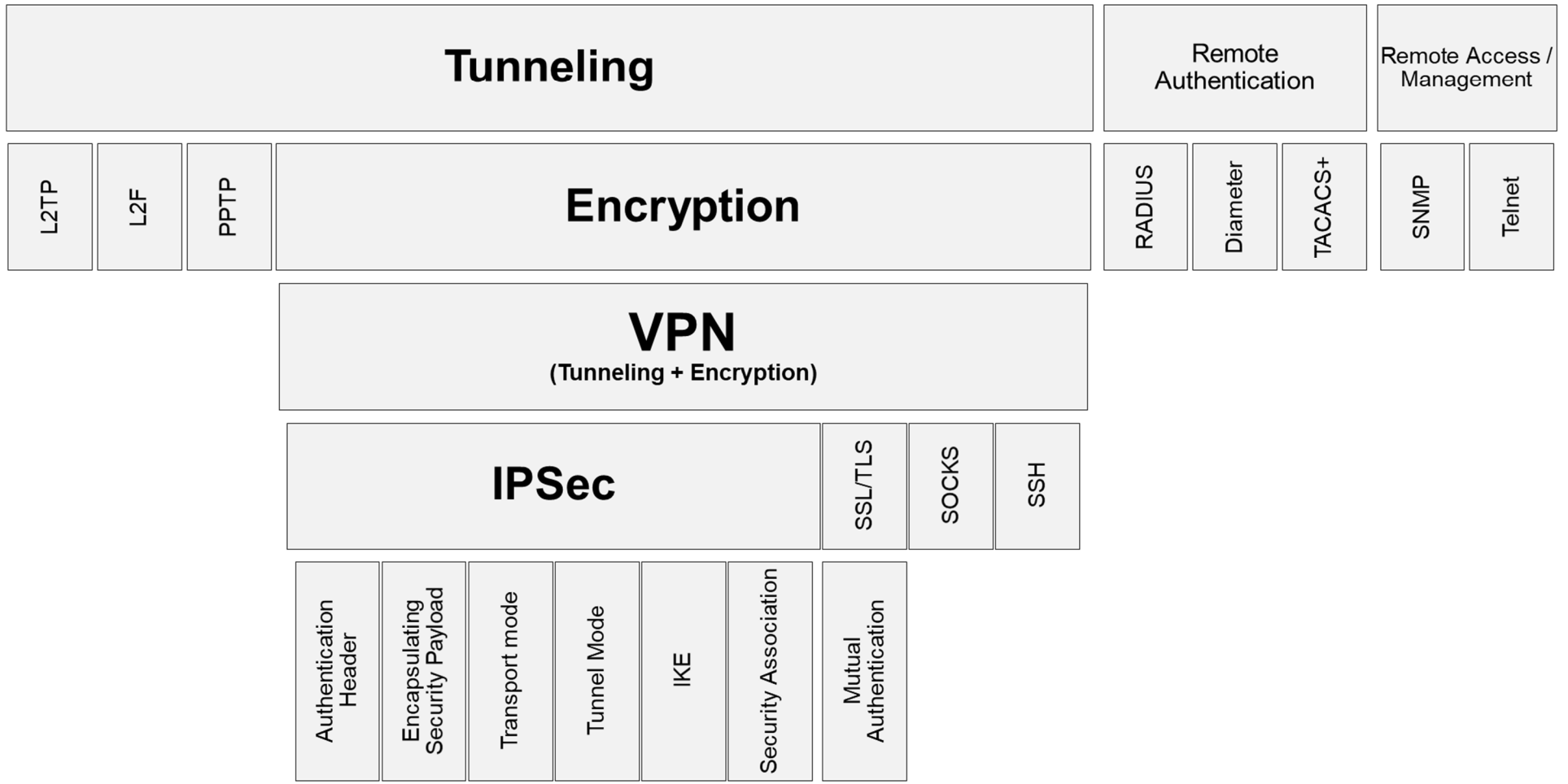
© 2019 Destination Certification Inc.

Network Defense

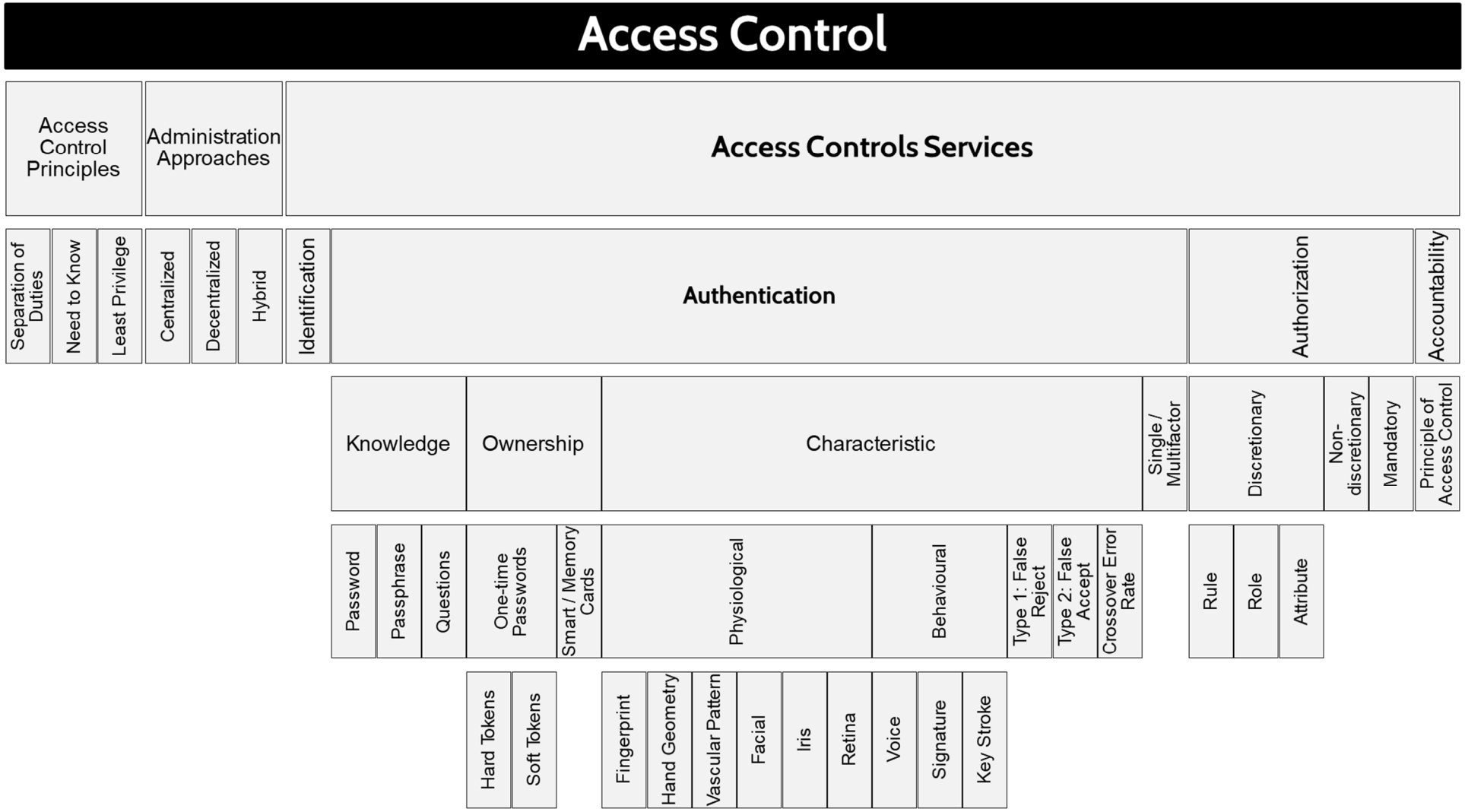
- **Defense in Depth**
- Network Segmentation / Partitioning
  - Network Perimeter
  - Choke Point
  - DMZ
  - Bastion Host
  - Proxy
  - NAT / PAT
- Firewalls
  - Types
    - Packet Filtering
    - Stateful Packet Filtering
    - Circuit Proxy
    - Application
  - Architectures
    - Packet Filtering
    - Dual-homed Host
    - Screened Host
    - Screened Subnet
    - 3-Legged Firewall
- Inspection
  - IDS
  - IPS
  - IDS/IPS Location
    - Host Based
    - Network Based
      - In-line
      - Mirror, Span, Promiscuous
  - IDS / IPS Detection Methods
    - Pattern
      - Signature analysis
    - Anomaly
      - Stateful matching
      - Statistical
      - Protocol
      - Traffic
    - White & Black lists
    - Sandbox
  - Honeypots & honeynets
    - Enticement vs. Entrapment
  - Ingress vs. Egress

© 2019 Destination Certification Inc.

Remote Access



© 2019 Destination Certification Inc.



© 2019 Destination Certification Inc.

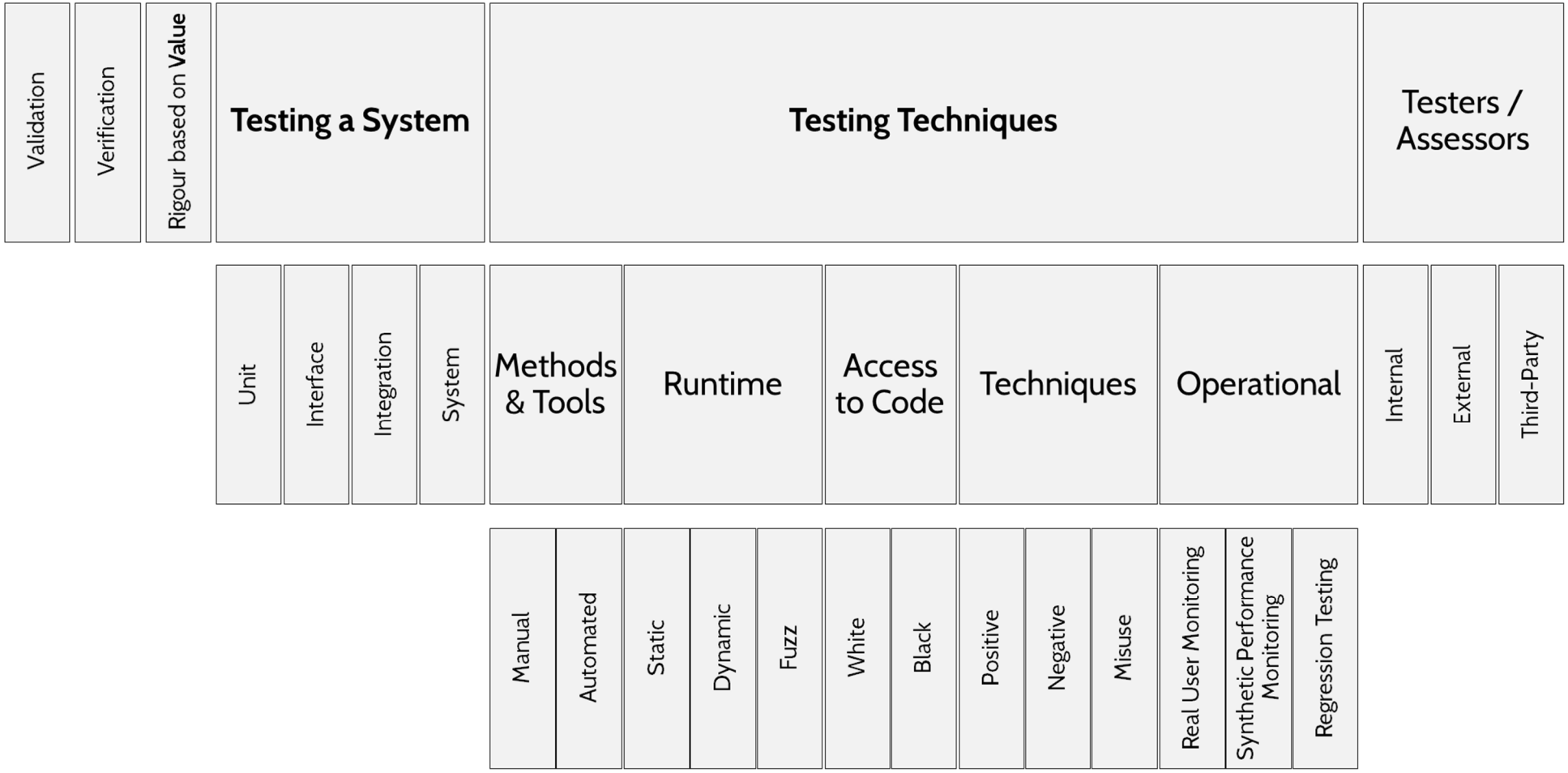
Single Sign-on / Federated Access

Allows users to access multiple systems with a single set of credentials

Single Sign-on		Federated Access					IDaaS
Access systems **only within the same organization**		Access systems across **multiple entities**					
Kerberos	Sesame	Trust Relationship			SAML		WS-Federation OpenID OAuth
One ticket	Symmetric encryption only	Multiple Tickets	Symmetric & Asymmetric encryption	Principal / User	Identity Provider	Relying Party / Service Provider	Tokens	Assertions written in XML

© 2019 Destination Certification Inc.

Security Assessment and Testing



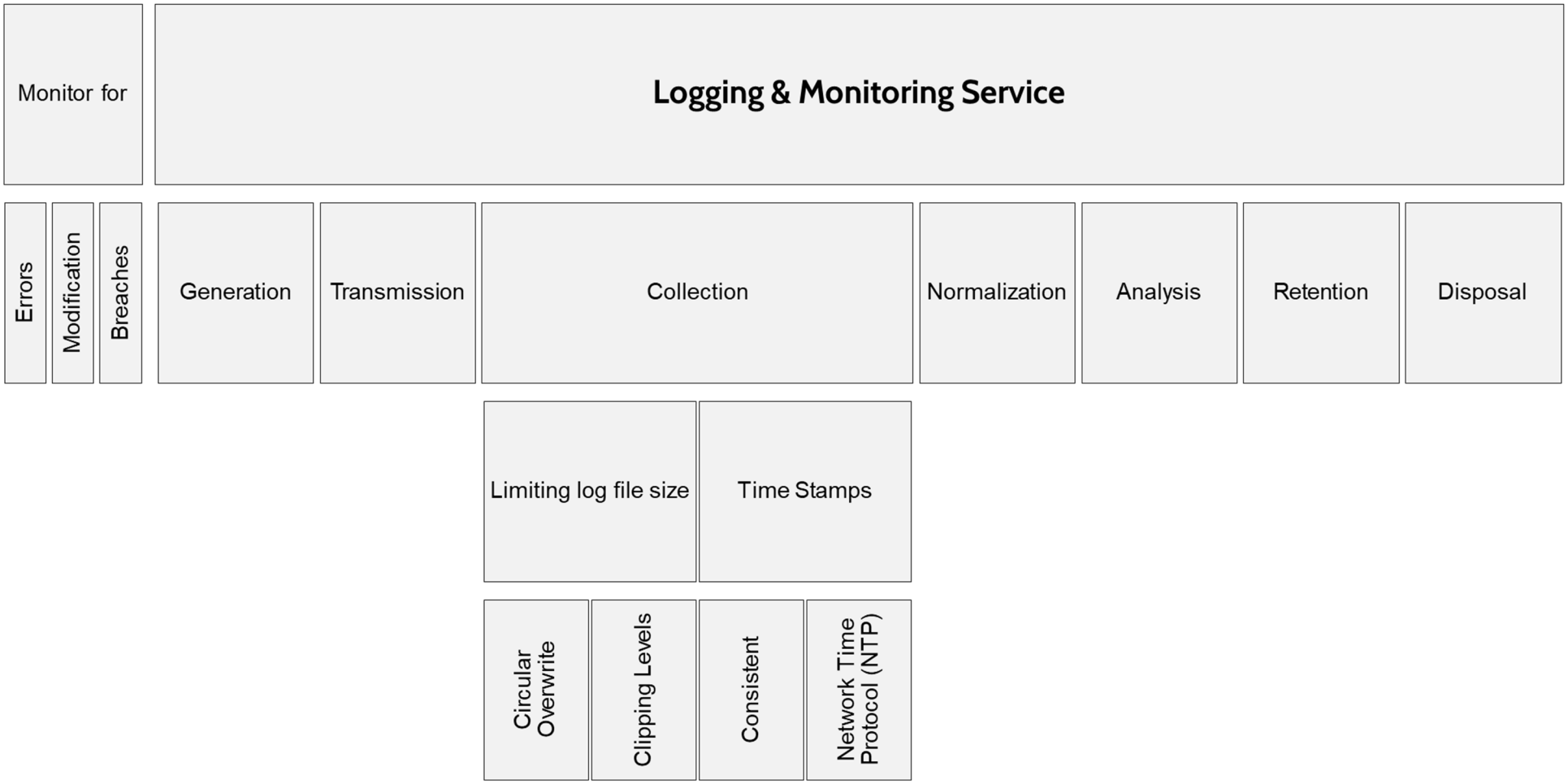
© 2019 Destination Certification Inc.

Identifying Vulnerabilities

- Vulnerability Assessment
- Penetration Test
- **Process**
  - Reconnaissance
  - Enumeration
  - Vulnerability Analysis
  - Execution
  - Document Findings
- **Testing Techniques**
  - Perspective
    - Internal
    - External
  - Approach
    - Blind
    - Double-blind
  - Knowledge
    - Zero (black)
    - Partial (gray)
    - Full (white)
- Types of Scans
  - Credentialed / Authenticated
  - Uncredentialed / Unauthenticated
- War dialing / War driving
- Banner grabbing & Fingerprinting
- Interpreting & understanding results
  - **CVE** Common Vulnerability & Exposures Dictionary
  - **CVSS** Common Vulnerability Scoring System
- False positive vs. False negative

© 2019 Destination Certification Inc.

Log Review & Analysis



© 2019 Destination Certification Inc.

Investigations

- **Secure the Scene**
- **Collect & Control Evidence**
  - **Locard's Principle**
  - **MOM**
  - Sources
    - Oral / Written statements
    - Documents
    - Digital Forensics
      - **Live Evidence (Volatile)**
      - Secondary Storage (HD)
    - E Discovery
  - **Chain of Custody**
- **Rules of Evidence**
  - Authentic
  - Accurate
  - Complete
  - Convincing
  - Admissible
- Investigative Techniques
  - Media Analysis
  - Software Analysis
  - Network Analysis
- Types of Investigations
  - Criminal
  - Civil
  - Regulatory
  - Administrative
- Document & Report

© 2019 Destination Certification Inc.

Security Information and Event Management (SIEM)

Capabilities						Continuously Update
Aggregation	Normalization	Correlation	Secure Storage	Analysis	Reporting	

Incident Response

Prep.	Triage		Action / Investigation		Recovery		
	Detection	Response IR Team Deployed	Mitigation Containment	Reporting Relevant Stakeholders	Recovery Return to normal	Remediation Prevention	Lessons Learned Improve Process

Sources: SIEM, IDS/IPS DLP, Fire detectors Etc.	Event	Incident

© 2019 Destination Certification Inc.

Incident Response

Preparation	Triage		Action / Investigation		Recovery		
	Detection	**Response** IR Team Deployed	**Mitigation** Containment	**Reporting** Relevant Stakeholders	**Recovery** Return to normal	**Remediation** Prevention	**Lessons Learned** Improve Process
	Sources: SIEM IDS/IPS DLP Anti-malware Cameras Fire detectors Etc.	Event	Incident				

© 2019 Destination Certification Inc.

Malware

Types

- Virus
- Worm
- Companion
- Macro
- Multipartite
- Polymorphic
- Trojan
- Botnets
- Hoaxes / Pranks
- Spyware / Adware
- Boot Sector Infector
- Logic Bombs
- Data Diddler / Salami Attack

Zero Day

Anti-Malware

- Policy
  - Training & Awareness
- Detection
  - Signature Based Scanners
  - Heuristic Scanners
  - Activity Monitors
  - Change Detection
- Continuous Updates

© 2019 Destination Certification Inc.

Patching

Determine if Patch is available				Implement through Change Management	
Threat Intelligence	Vendor Notification	Pro-actively checking		Deploy	
		Agent	Agentless	Passive	Automated	Manual

Change Management

Change Request	Assess Impact	Approval	Build & Test	Notification	Implement	Validation		Version & Baseline
	Emergency Change vs. Standard process	Based on impact, severity, etc.				Test New Functionality	Regression Testing	

© 2019 Destination Certification Inc.

Recovery Strategies

Backup Storage

- Archive Bit
- Types of Backups
  - Mirror
  - Full
  - Incremental
  - Differential
- Data Storage
  - Offsite
  - Tape Rotation

Spare Parts

- Cold
- Warm
- Hot

RAID

Redundant Array of Independent Disks

- **RAID 0** Striping
- **RAID 1** Mirroring
- **RAID 5** Parity

High Availability System

- Clustering
- Redundancy

Recovery Sites

- Types of Sites
  - Cold
  - Warm
  - Hot
  - Mobile
  - Redundant
- Geographically remote
- Reciprocal Agreements

© 2019 Destination Certification Inc.

Business Continuity Management (BCM)

Focuses on **critical and essential functions** of business

Goals of BCM

1. Safety of people
2. Minimize damage
3. Survival of business

Business Impact Assessment

- Identify Critical Processes & Systems
- Measurements of Time
  - **RPO**
  - **RTO**
  - **WRT**
  - **MTD**
- Owner approval of #s and associated costs

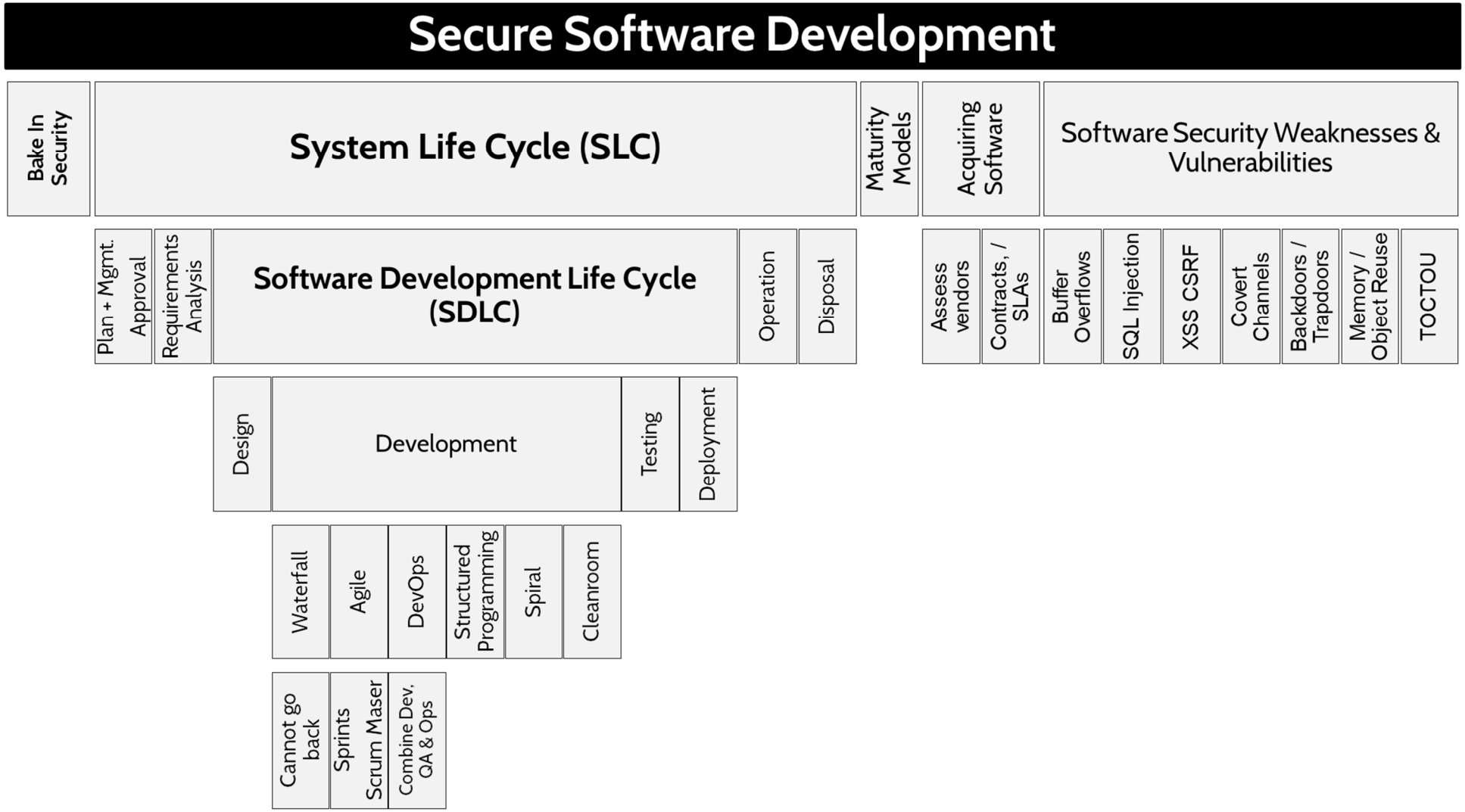
Types of Plans

- Business Continuity Plan (**BCP**)
- Disaster Recovery Plan (**DRP**)

Testing Plans

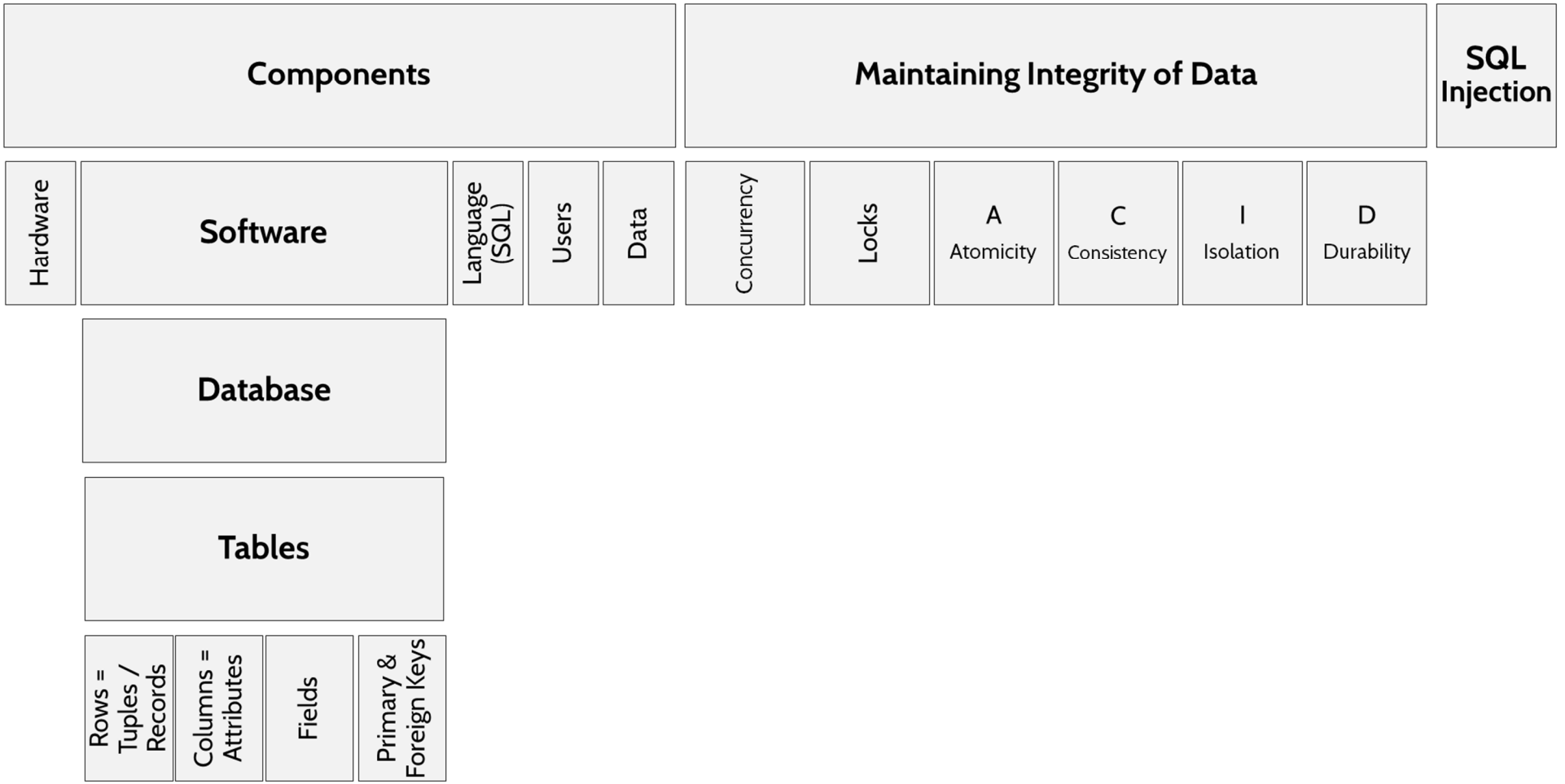
- Read-through / Checklist
- Walkthrough
- Simulation
- Parallel
- Full-interruption / Full-scale

© 2019 Destination Certification Inc.



© 2019 Destination Certification Inc.

Databases



© 2019 Destination Certification Inc.