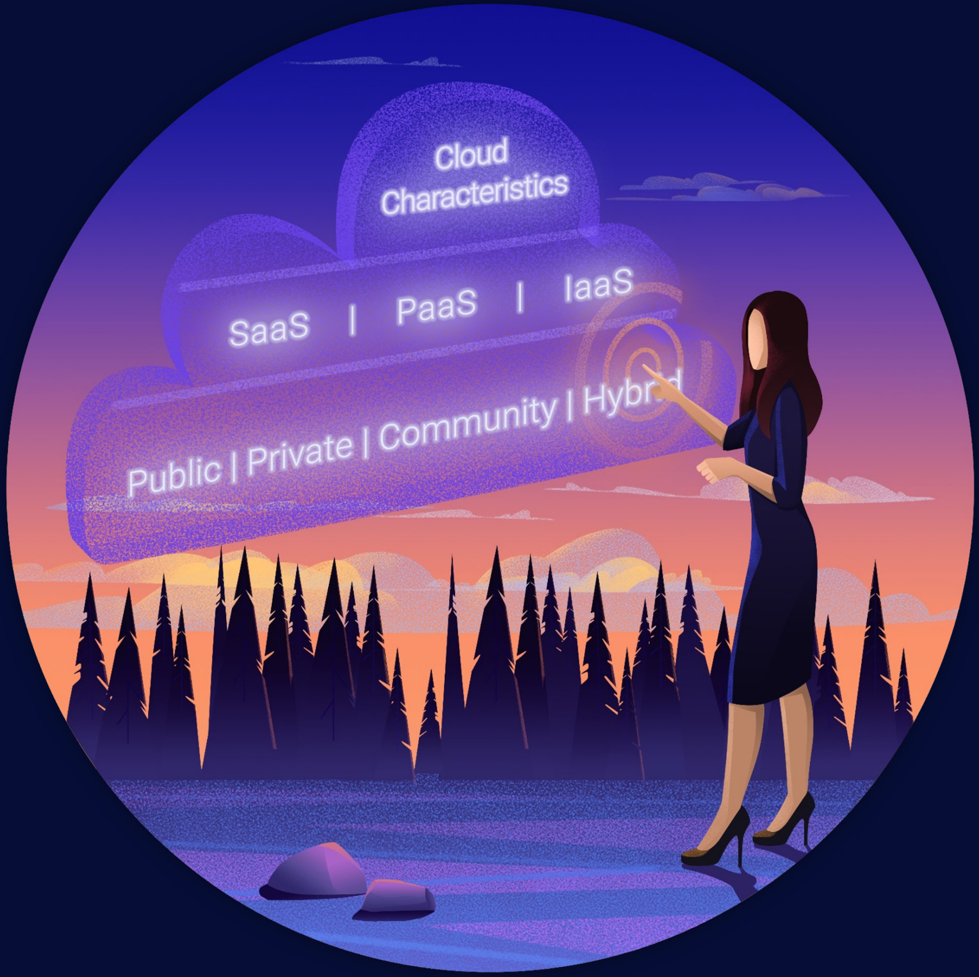
DESTINATION
CERTIFICATION

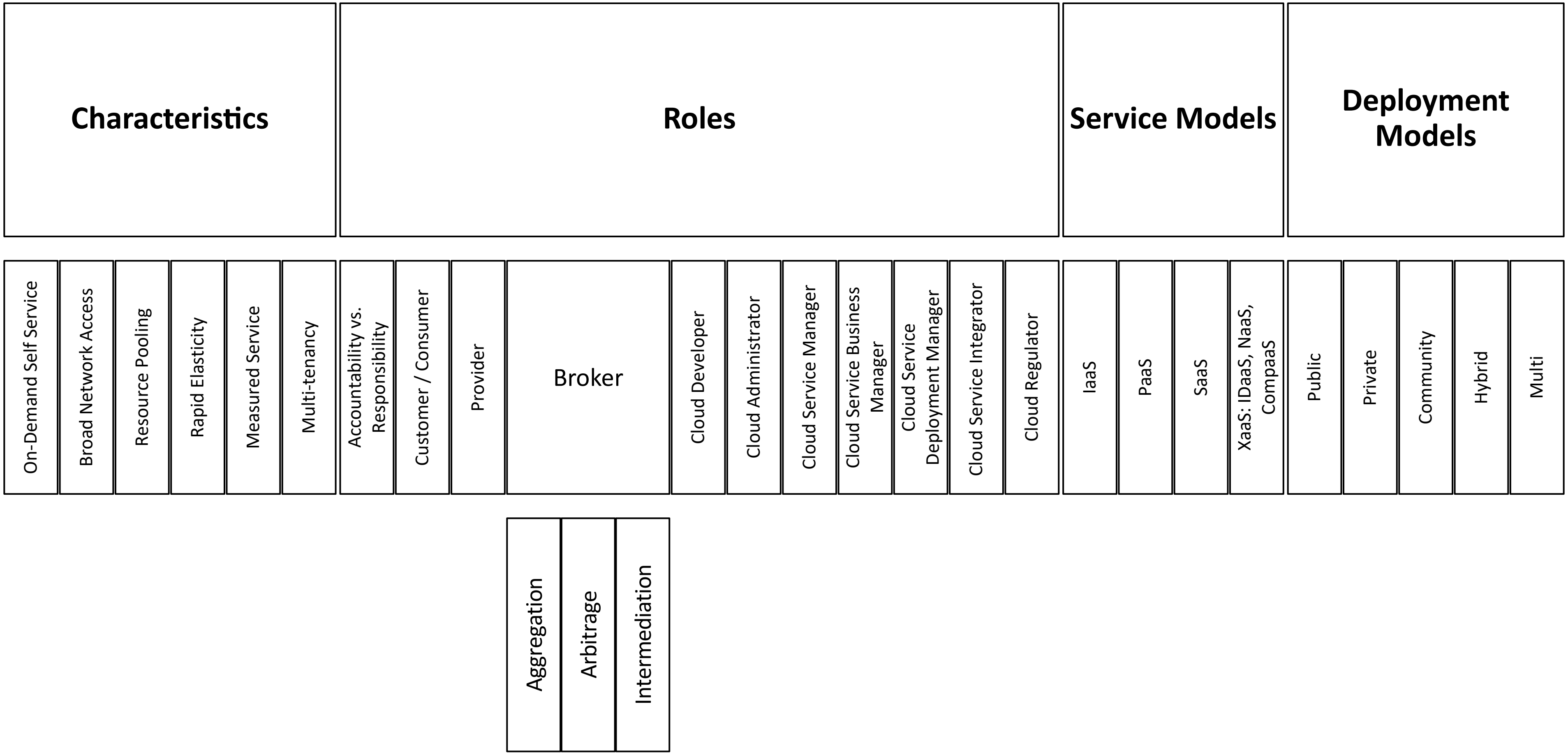
CCSP MindMaps



1

Cloud Concepts, Architecture and Design

Cloud Computing



Characteristics

- On-Demand Self Service
- Broad Network Access
- Resource Pooling
- Rapid Elasticity
- Measured Service
- Multi-tenancy

Roles

- Accountability vs. Responsibility
- Customer / Consumer
- Provider
- Broker
  - Aggregation
  - Arbitrage
  - Intermediation
- Cloud Developer
- Cloud Administrator
- Cloud Service Manager
- Cloud Service Business Manager
- Cloud Service Deployment Manager
- Cloud Service Integrator
- Cloud Regulator

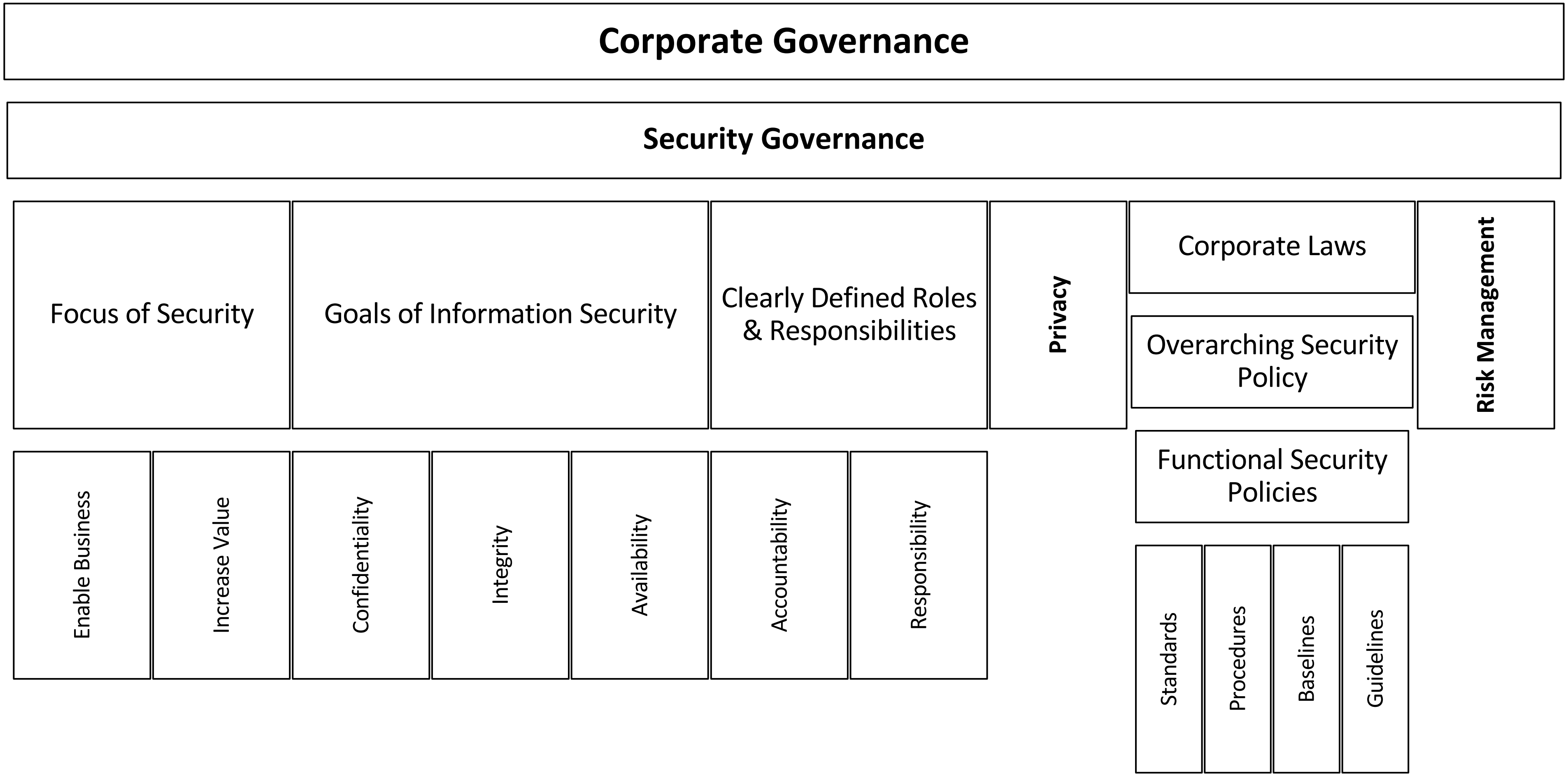
Service Models

- IaaS
- PaaS
- SaaS
- XaaS: IDaaS, NaaS, CompaaS

Deployment Models

- Public
- Private
- Community
- Hybrid
- Multi

Alignment of Security Function to Business Strategy



Corporate Governance

Security Governance

Focus of Security

Enable Business

Increase Value

Goals of Information Security

Confidentiality

Integrity

Availability

Clearly Defined Roles & Responsibilities

Accountability

Responsibility

Privacy

Corporate Laws

Overarching Security Policy

Functional Security Policies

Standards

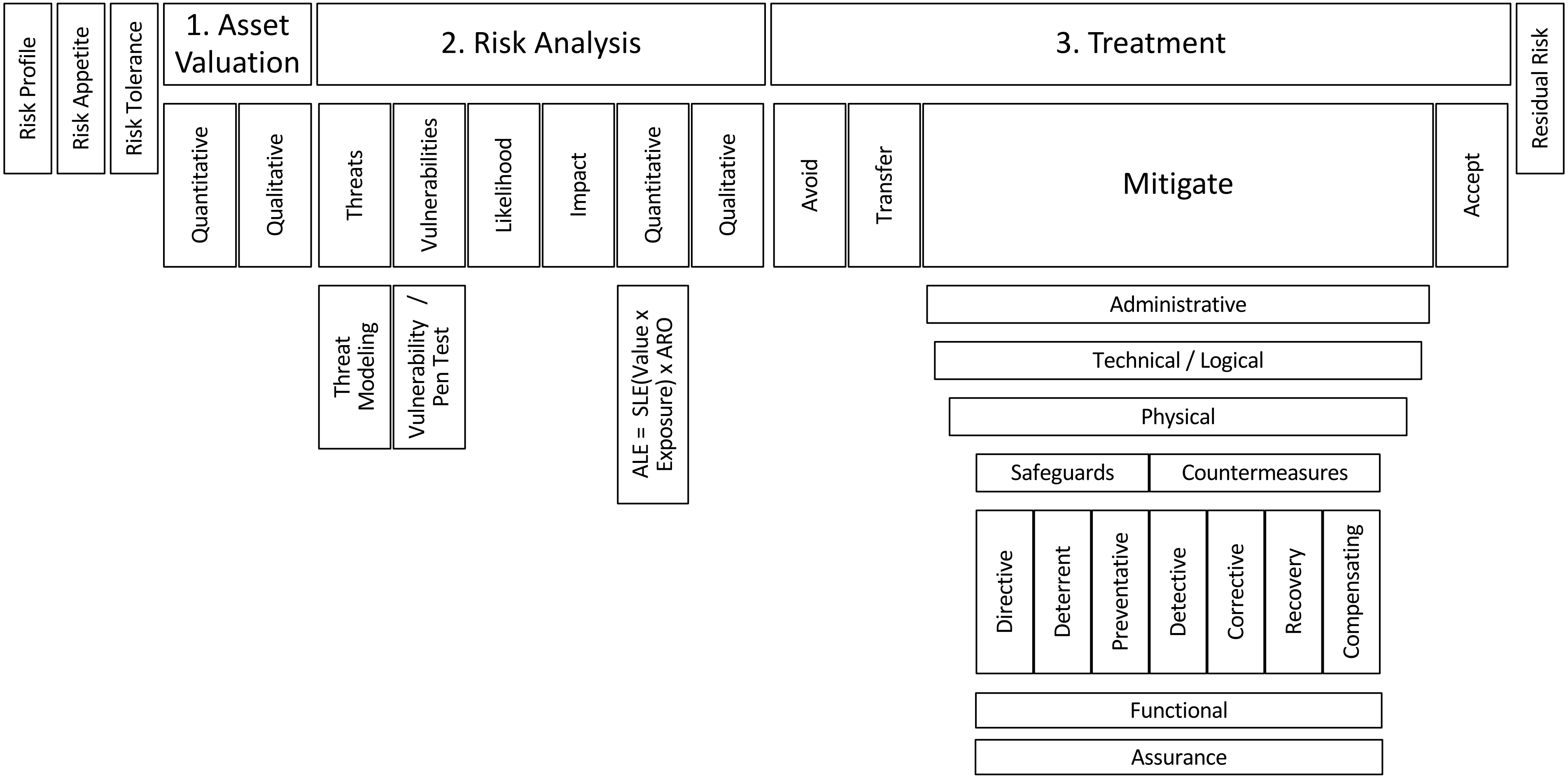
Procedures

Baselines

Guidelines

Risk Management

Risk Management



Risk Profile

Risk Appetite

Risk Tolerance

1. Asset Valuation
- Quantitative
- Qualitative

2. Risk Analysis
- Threats
  - Threat Modeling
- Vulnerabilities
  - Vulnerability / Pen Test
- Likelihood
- Impact
- Quantitative
  - ALE = SLE(Value x Exposure) x ARO
- Qualitative

3. Treatment
- Avoid
- Transfer
- Mitigate
  - Administrative
  - Technical / Logical
  - Physical
  - Safeguards
  - Countermeasures
  - Directive
  - Deterrent
  - Preventative
  - Detective
  - Corrective
  - Recovery
  - Compensating
  - Functional
  - Assurance
- Accept

Residual Risk

Cloud Shared Considerations

Cloud must be a business decision

- Interoperability
- **Data** Portability
- Application Portability
- Reversibility
- Availability
- Security
- Privacy
- Resiliency
- Performance
- Governance
- Service Level Agreements (SLAs)
- Auditability
- Regulatory

Frameworks

Provide **Comprehensive Guidance**

Security Control Frameworks		**Cloud** Security Control Frameworks			**Cloud Design Patterns**			**Risk Frameworks**				
ISO 27001	ISO 27002	CSA Cloud Controls Matrix (CCM)	ISO 27017	ISO 27018	SANS security principles	Well-Architected Framework	CSA Enterprise Architecture	ISO 31000	ENISA	CSA	NIST	Microsoft

Cost Benefit Analysis

- Pay per usage
- CapEx to OpEx
- Depreciation
- Datacenter / utility costs
- Resource pooling
- Software licensing
- Personnel & operational costs
- Shift in focus

Evaluation Criteria

Certification

Common Criteria

EAL1 – EAL7

FIPS 140-2

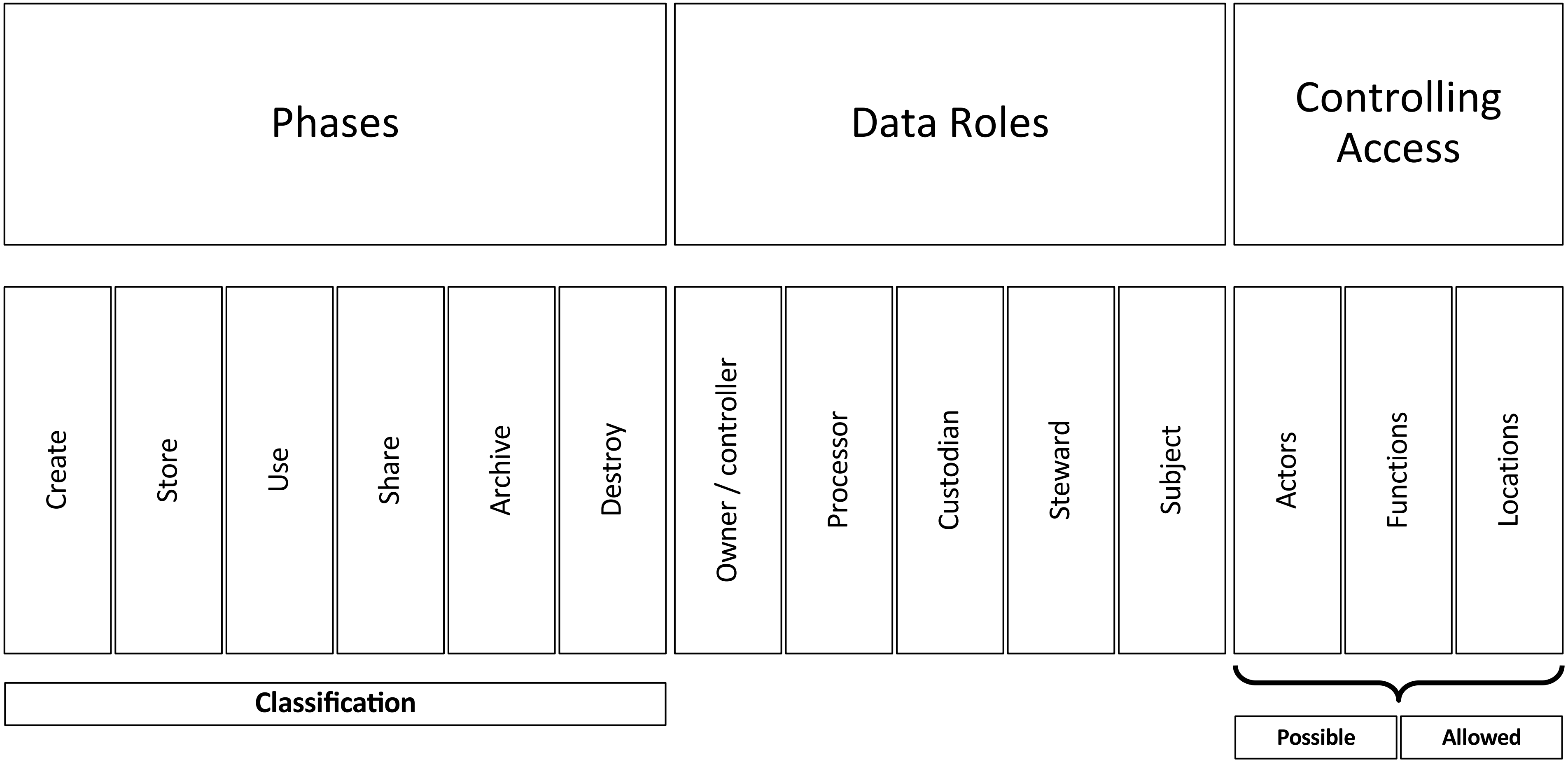
Levels 1 - 4

Accreditation

2

Cloud Data Security

Cloud Data Lifecycle



Phases

Create

Store

Use

Share

Archive

Destroy

Classification

Data Roles

Owner / controller

Processor

Custodian

Steward

Subject

Controlling Access

Actors

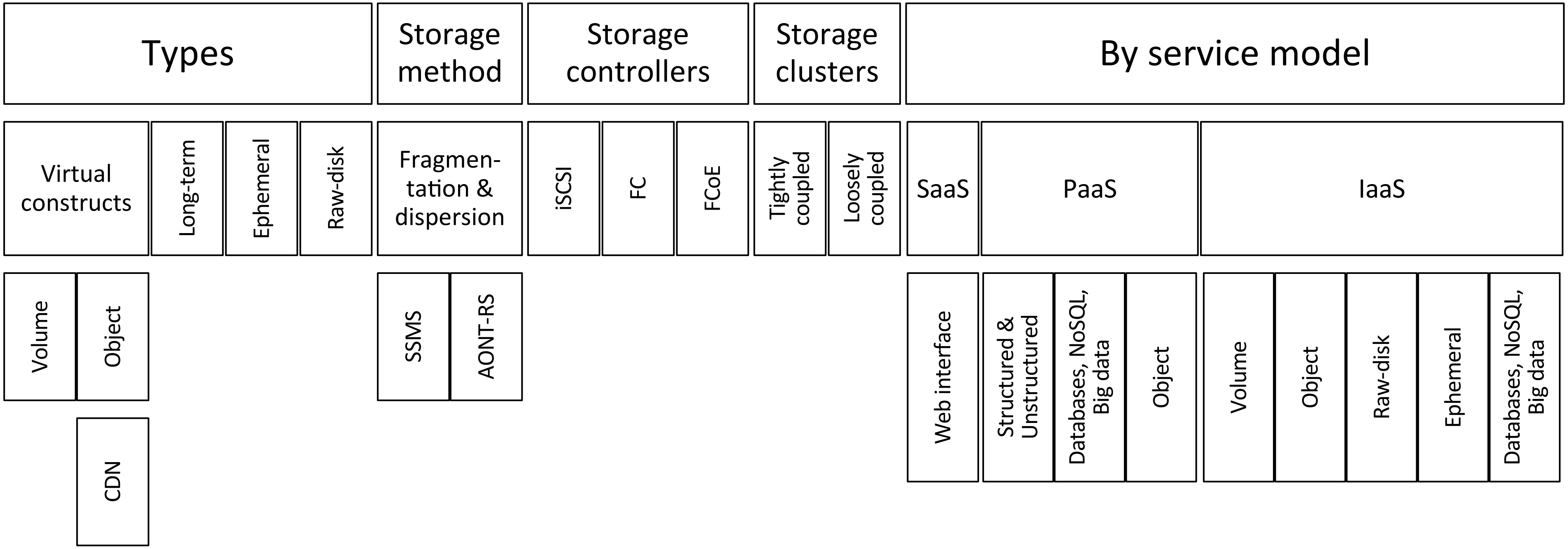
Functions

Locations

Possible

Allowed

Cloud Data Storage

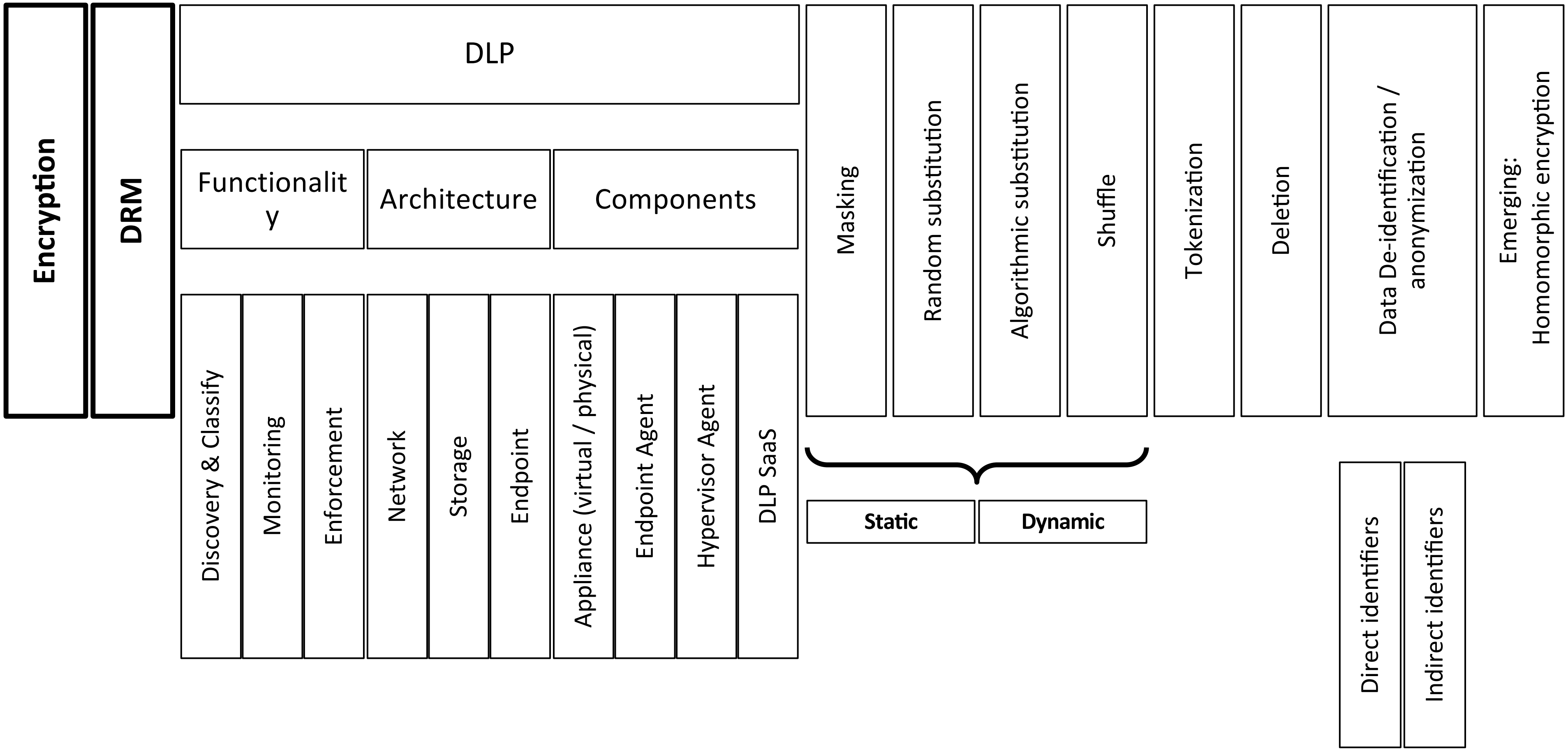


- Types
  - Virtual constructs
    - Volume
    - Object
      - CDN
  - Long-term
  - Ephemeral
  - Raw-disk
- Storage method
  - Fragmentation & dispersion
    - SSMS
    - AONT-RS
- Storage controllers
  - iSCSI
  - FC
  - FCoE
- Storage clusters
  - Tightly coupled
  - Loosely coupled
- By service model
  - SaaS
    - Web interface
  - PaaS
    - Structured & Unstructured
    - Databases, NoSQL, Big data
    - Object
  - IaaS
    - Volume
    - Object
    - Raw-disk
    - Ephemeral
    - Databases, NoSQL, Big data

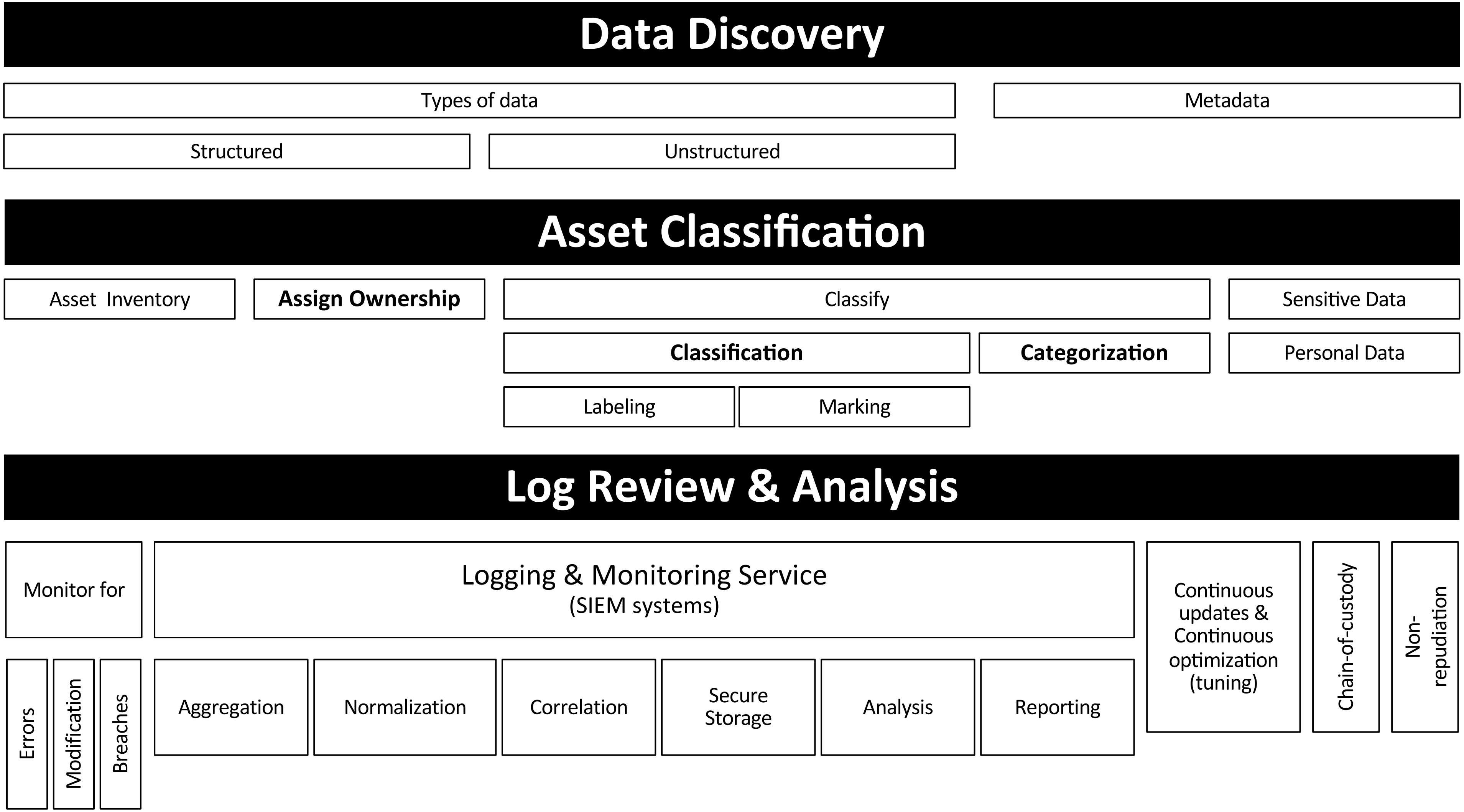
Threats to Storage

- Unauthorized usage
- Unauthorized access
- Regulatory non-compliance
- Denial of Service (DoS)
- Theft or accidental loss
- Malware
- No sanitization

Data Security Strategies



- **Encryption**
- **DRM**
- DLP
  - Functionality
    - Discovery & Classify
    - Monitoring
    - Enforcement
  - Architecture
    - Network
    - Storage
    - Endpoint
  - Components
    - Appliance (virtual / physical)
    - Endpoint Agent
    - Hypervisor Agent
    - DLP SaaS
- Masking
- Random substitution
- Algorithmic substitution
- Shuffle
  - **Static**
  - **Dynamic**
- Tokenization
- Deletion
- Data De-identification / anonymization
  - Direct identifiers
  - Indirect identifiers
- Emerging: Homomorphic encryption



Data Discovery

Types of data

Structured

Unstructured

Metadata

Asset Classification

Asset Inventory

Assign Ownership

Classify

Classification

Labeling

Marking

Categorization

Sensitive Data

Personal Data

Log Review & Analysis

Monitor for

Errors

Modification

Breaches

Logging & Monitoring Service
(SIEM systems)

Aggregation

Normalization

Correlation

Secure Storage

Analysis

Reporting

Continuous updates & Continuous optimization (tuning)

Chain-of-custody

Non-repudiation

Digital Rights Management (DRM)

Consumer DRM

Enterprise DRM

Information Rights Management (IRM)

- Auditing of access / use
- Signing / sealing
- Rights based on classification
- Controlling copy & pasting, screenshots

Cloud DRM Challenges

Data Retention, Archiving & Deletion

Data retention policies

Migration to slower storage

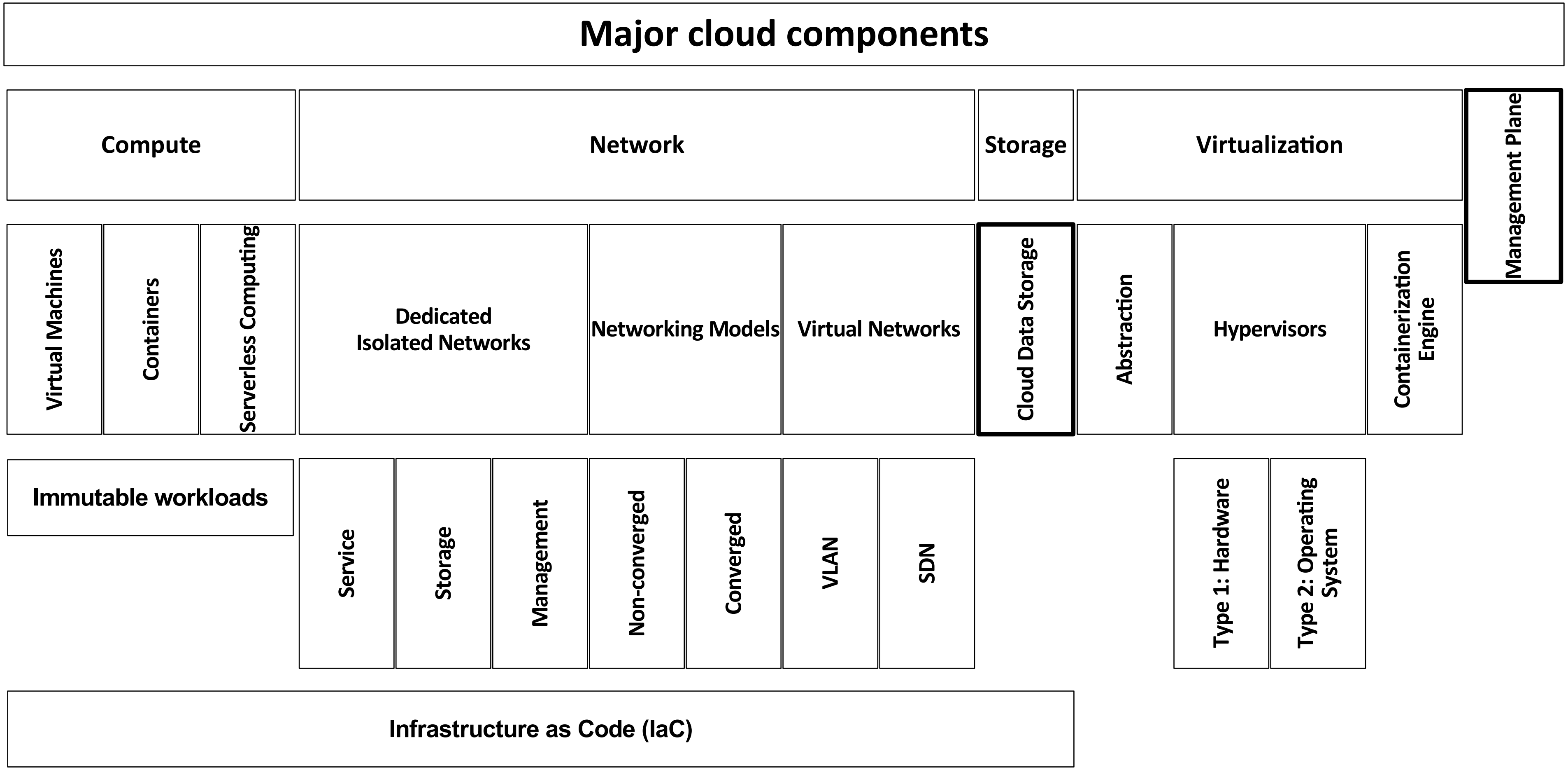
Defensible Destruction

- Destruction
  - Media Destruction
  - Shred / Disintegrate / Drill
- Purging
  - Degauss
  - Crypto shredding
- Clearing
  - Overwrite / Wipe / Erasure
  - Format

3

Cloud Platform and Infrastructure Security

Cloud Infrastructure Components

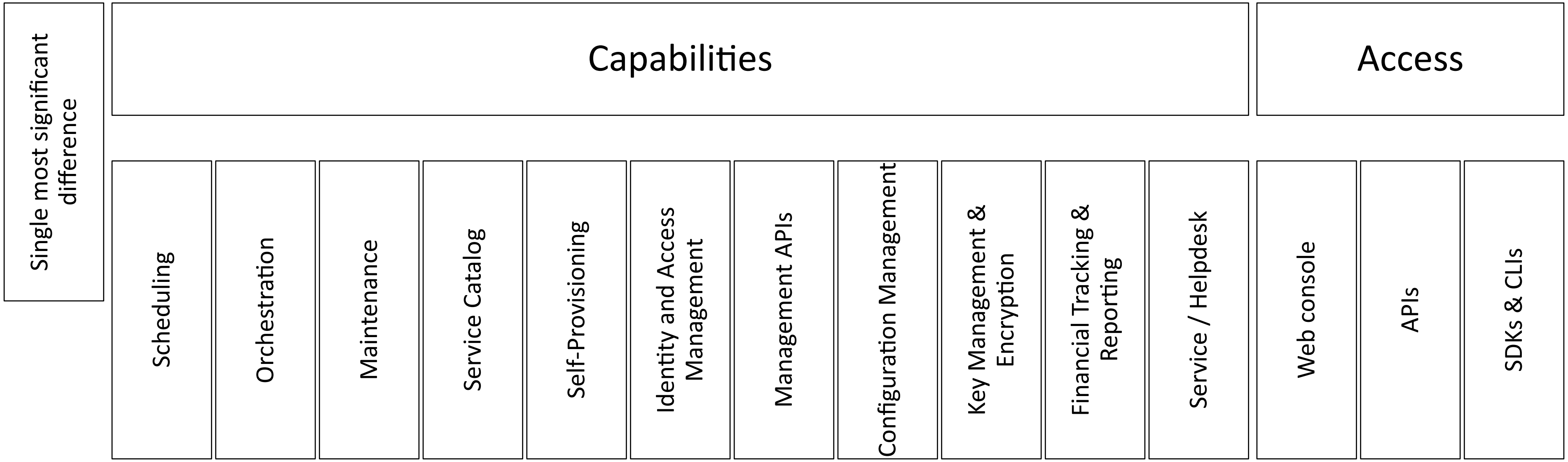


Major cloud components

- Compute
  - Virtual Machines
  - Containers
  - Serverless Computing
  - Immutable workloads
- Network
  - Dedicated Isolated Networks
    - Service
    - Storage
    - Management
  - Networking Models
    - Non-converged
    - Converged
  - Virtual Networks
    - VLAN
    - SDN
- Storage
  - Cloud Data Storage
- Virtualization
  - Abstraction
  - Hypervisors
    - Type 1: Hardware
    - Type 2: Operating System
  - Containerization Engine
- Management Plane

Infrastructure as Code (IaC)

Management Plane



Single most significant difference

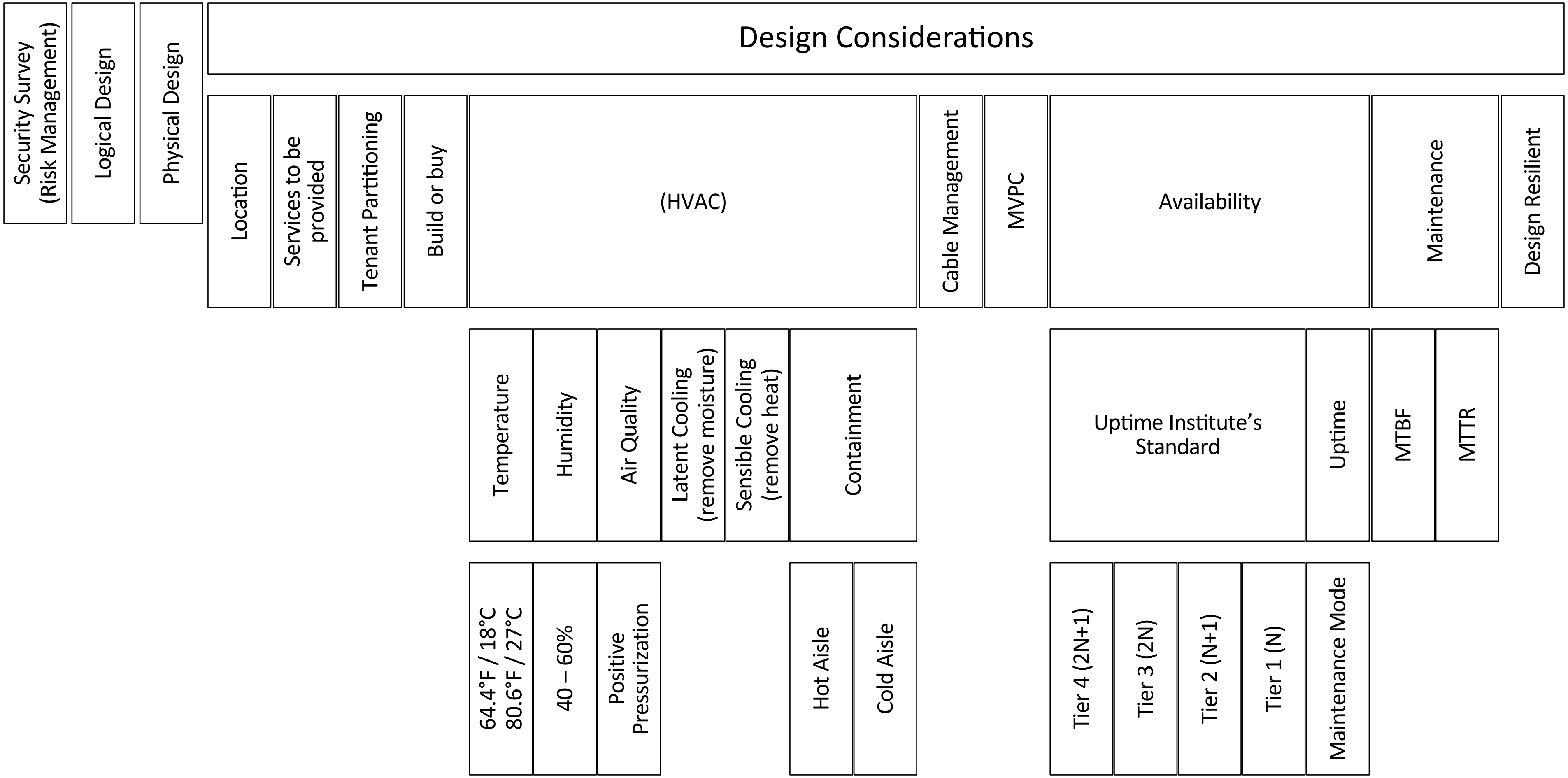
Capabilities

- Scheduling
- Orchestration
- Maintenance
- Service Catalog
- Self-Provisioning
- Identity and Access Management
- Management APIs
- Configuration Management
- Key Management & Encryption
- Financial Tracking & Reporting
- Service / Helpdesk

Access

- Web console
- APIs
- SDKs & CLIs

Data Center Design



Security Survey (Risk Management)

Logical Design

Physical Design

Design Considerations

Location

Services to be provided

Tenant Partitioning

Build or buy

(HVAC)

Temperature

64.4°F / 18°C
80.6°F / 27°C

Humidity

40 – 60%

Air Quality

Positive Pressurization

Latent Cooling (remove moisture)

Sensible Cooling (remove heat)

Containment

Hot Aisle

Cold Aisle

Cable Management

MVPC

Availability

Uptime Institute's Standard

Tier 4 (2N+1)

Tier 3 (2N)

Tier 2 (N+1)

Tier 1 (N)

Uptime

Maintenance Mode

Maintenance

MTBF

MTTR

Design Resilient

Attack Vectors

Common

- Denial of Service
- Malware
- System vulnerabilities
- XSS, CSRF, SQL Injection, etc.
- Malicious insiders
- Social engineering
- Advanced Persistent Threats

Specific to Cloud

- Insufficient Due Diligence
- Guest Escape / VM Hopping
- Hyperjacking attack
- Hyperstack attack
- Insecure Interfaces / APIs
- Provider's infrastructure
- Shared technology
- Account hijacking

Risks

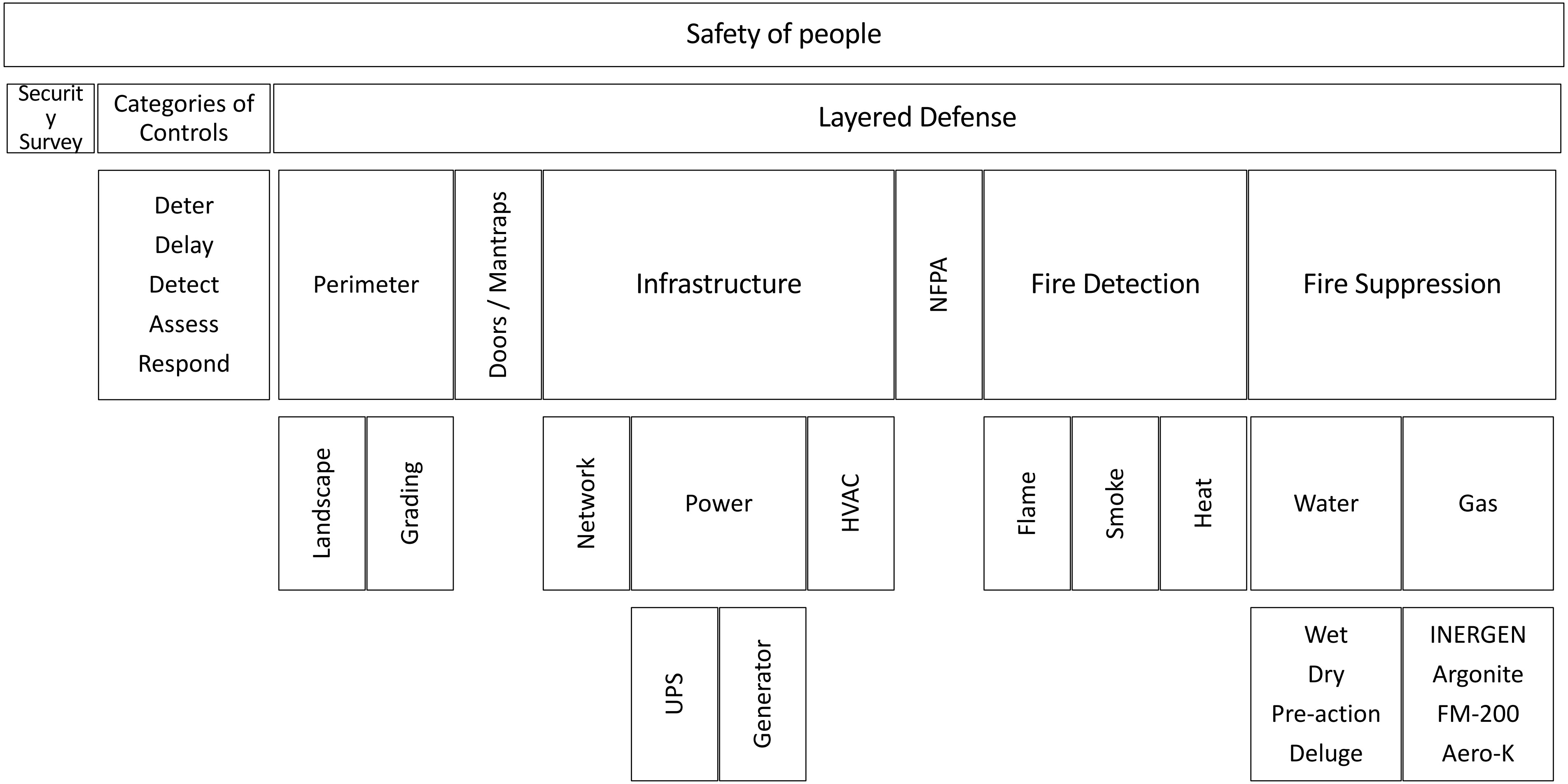
Common

- Data Loss / Breach
- Data Integrity
- Compliance & regulatory

Specific to Cloud

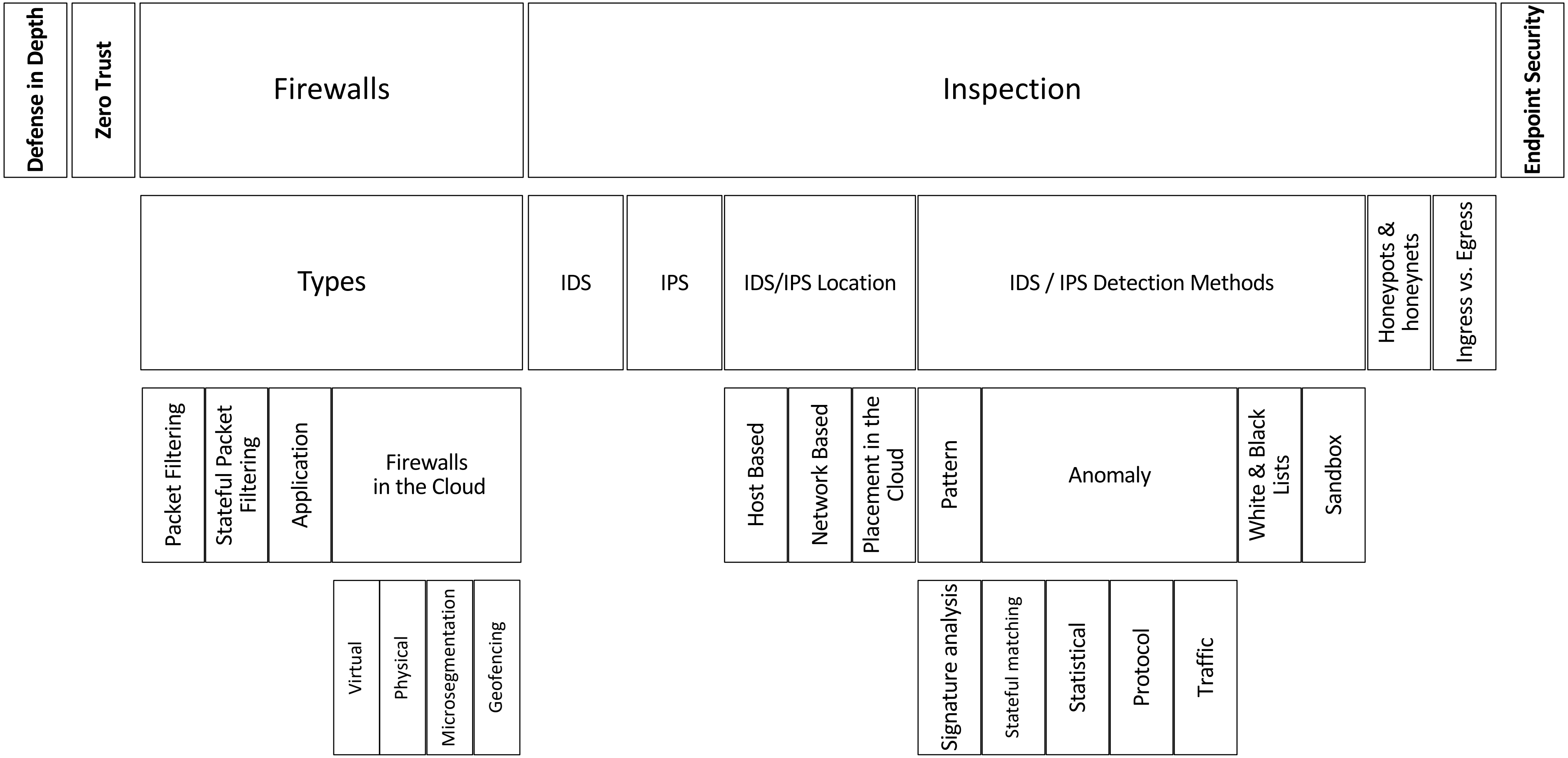
- VM Sprawl
- Sensitive data within a VM
- Dormant VMs
- Instant-on gaps
- Resource exhaustion
- Hypervisor security
- Data comingling
- Inter-VM communication (blindspots)

Physical Security



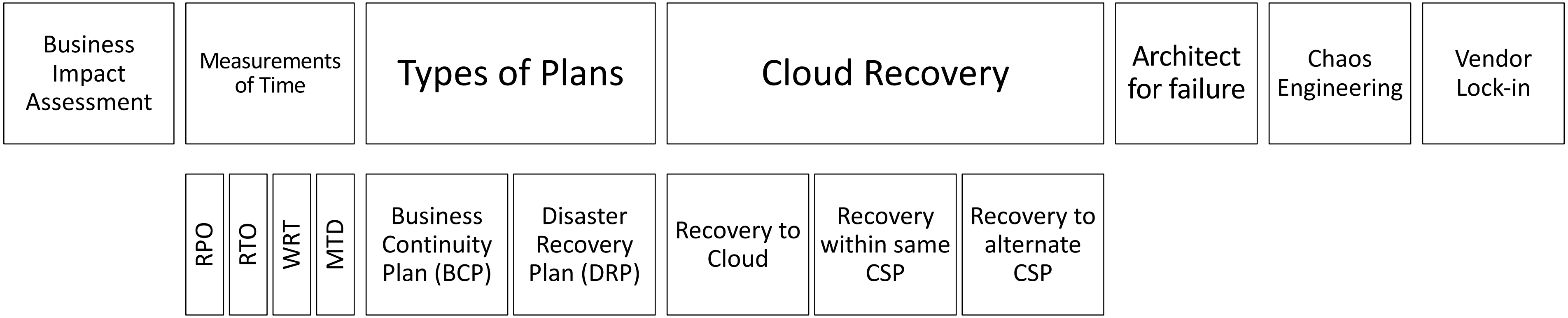
- Safety of people
- Security Survey
- Categories of Controls
  - Deter
  - Delay
  - Detect
  - Assess
  - Respond
- Layered Defense
  - Perimeter
    - Landscape
    - Grading
  - Doors / Mantraps
  - Infrastructure
    - Network
    - Power
      - UPS
      - Generator
    - HVAC
  - NFPA
  - Fire Detection
    - Flame
    - Smoke
    - Heat
  - Fire Suppression
    - Water
      - Wet
      - Dry
      - Pre-action
      - Deluge
    - Gas
      - INERGEN
      - Argonite
      - FM-200
      - Aero-K

Network Defense



- Defense in Depth
- Zero Trust
- Firewalls
  - Types
    - Packet Filtering
    - Stateful Packet Filtering
    - Application
    - Firewalls in the Cloud
      - Virtual
      - Physical
      - Microsegmentation
      - Geofencing
- Inspection
  - IDS
  - IPS
  - IDS/IPS Location
    - Host Based
    - Network Based
    - Placement in the Cloud
  - IDS / IPS Detection Methods
    - Pattern
      - Signature analysis
    - Anomaly
      - Stateful matching
      - Statistical
      - Protocol
      - Traffic
    - White & Black Lists
    - Sandbox
  - Honeypots & honeynets
  - Ingress vs. Egress
- Endpoint Security

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)

Cloud Recovery

- Recovery to Cloud
- Recovery within same CSP
- Recovery to alternate CSP

Architect for failure

Chaos Engineering

Vendor Lock-in

4

Cloud Application Security

Cloud Development

- OWASP Top 10
- SANS / CWE Top 25

Common Pitfalls

- On-premise may not transfer
- New knowledge & skills required
- Different risk profiles
- Integration complexity
- Legacy applications
- Multitenancy

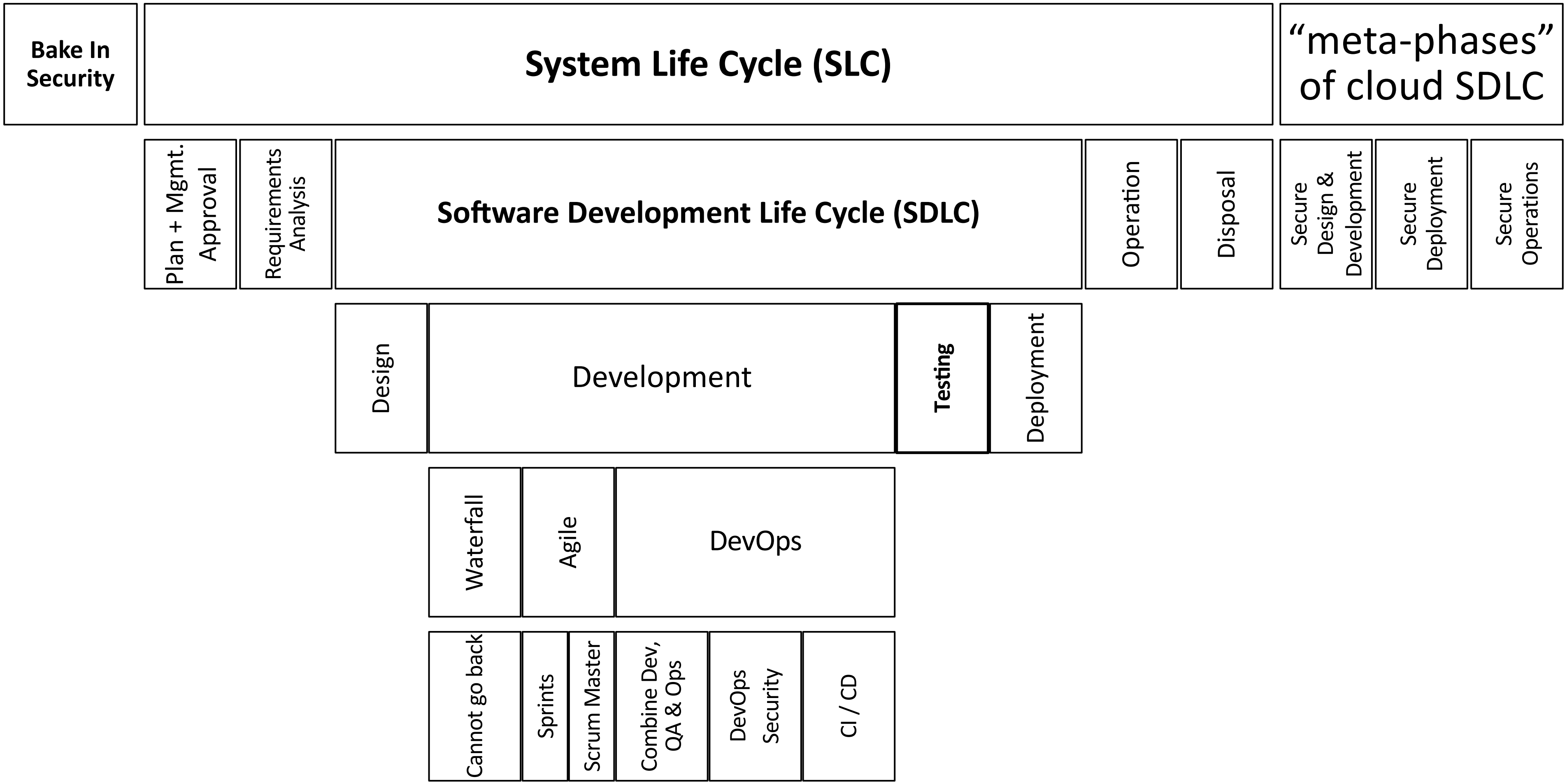
Opportunities

- Higher baseline security
- Responsiveness
- Isolated environments
- Micro-service architectures
- Elasticity
- DevOps
- Unified management interface
- Immutable infrastructure

Challenges

- Limited logging visibility
- Increased application scope
- Changing threat models
- Reduced transparency

Secure Software Development



Bake In Security

System Life Cycle (SLC)

Plan + Mgmt. Approval

Requirements Analysis

Software Development Life Cycle (SDLC)

Design

Development

Waterfall

Cannot go back

Agile

Sprints

Scrum Master

DevOps

Combine Dev, QA & Ops

DevOps Security

CI / CD

Testing

Deployment

Operation

Disposal

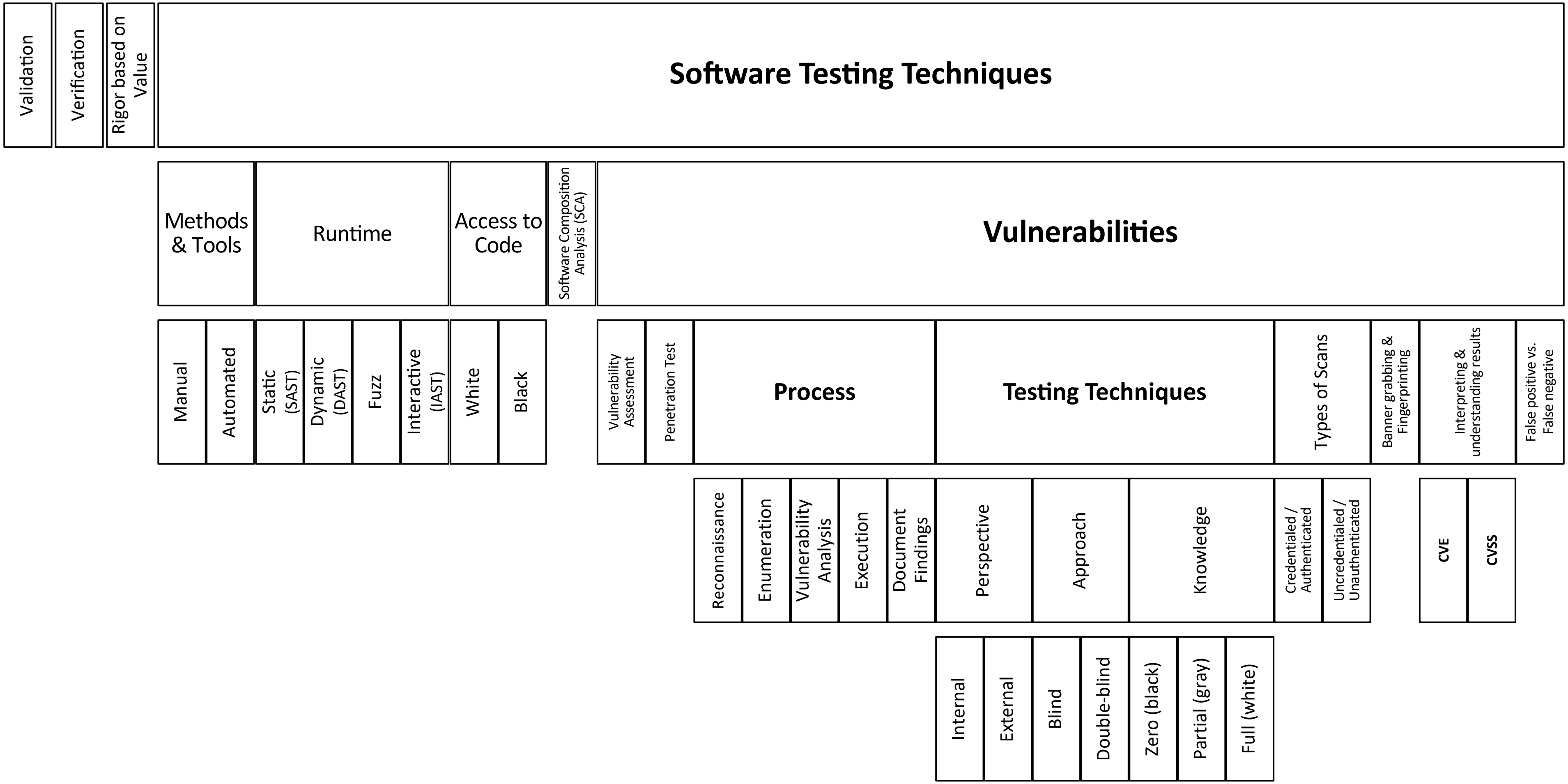
“meta-phases” of cloud SDLC

Secure Design & Development

Secure Deployment

Secure Operations

Security Assessment and Testing



Validation

Verification

Rigor based on Value

Software Testing Techniques

- Methods & Tools
  - Manual
  - Automated
- Runtime
  - Static (SAST)
  - Dynamic (DAST)
  - Fuzz
  - Interactive (IAST)
- Access to Code
  - White
  - Black
- Software Composition Analysis (SCA)
- 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
  - Banner grabbing & Fingerprinting
  - Interpreting & understanding results
    - CVE
    - CVSS
  - False positive vs. False negative

Common Vulnerabilities & Threat Modeling

Cross Site Scripting (XSS)

Cross Site Request Forgery (CSRF)

SQL Injection

Insecure Direct Object Reference

Buffer Overflow

Threat Modeling

Stored (Persistent)

Reflected

DOM

Parameter / bounds checking

ATASM

STRIDE

PASTA

DREAD

Input Validation

Verified Secure Software

Application Programming Interfaces (APIs)

Approved APIs

Software / API Supply chain management

REST

SOAP

Simple
Fast
Most Widely Used

More capabilities
More complexity

Cryptographic Services

Confidentiality

Integrity

= Hashing

Authenticity

Non-Repudiation

Origin

Delivery

Access Control

Cryptography

One-way

Hashing

Two-way

Symmetric

Asymmetric

Digital Signatures

Integrity
Authenticity
Non-repudiation

Digital Certificates

Verify owner of public key

X.509

Key Management

Kirchhoff’s Law

Generation

Distribution

Out-of-band
Hybrid

Storage

TPM
HSM

Rotation

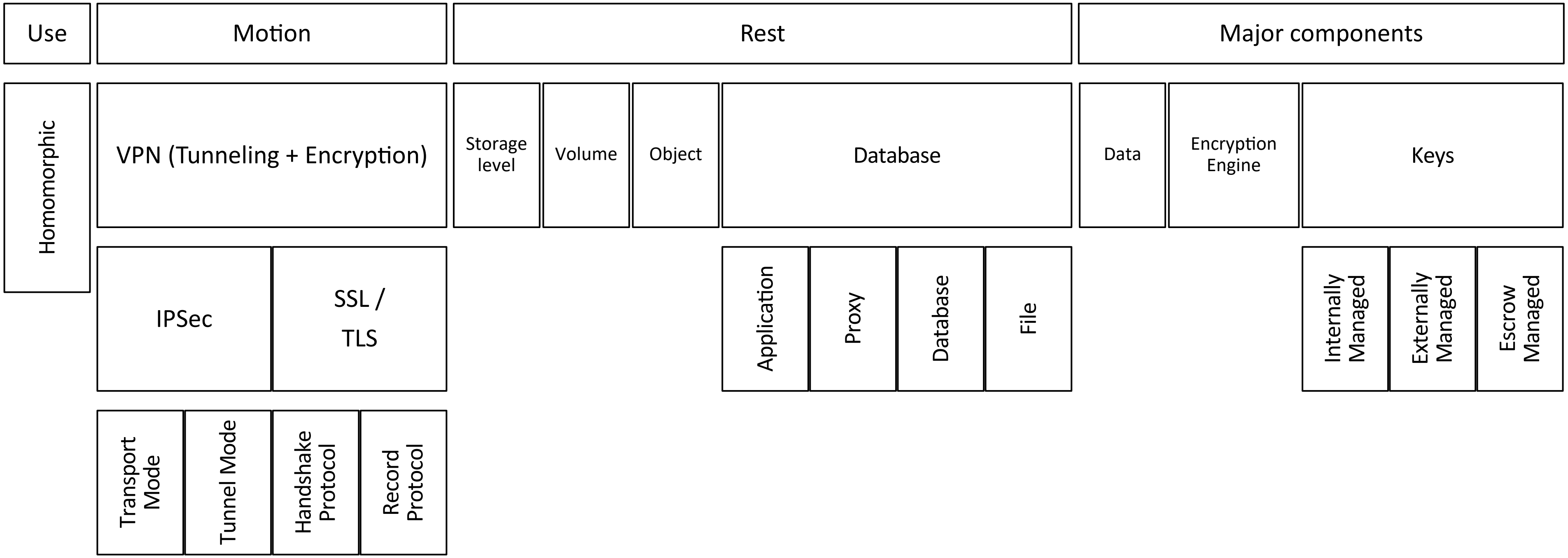
Disposition

Crypto-shredding
Key Destruction

Recovery

Split Knowledge
Dual Control
Key Escrow

Crypto in the Clouds



- Use
  - Homomorphic
- Motion
  - VPN (Tunneling + Encryption)
    - IPSec
      - Transport Mode
      - Tunnel Mode
    - SSL / TLS
      - Handshake Protocol
      - Record Protocol
- Rest
  - Storage level
  - Volume
  - Object
  - Database
    - Application
    - Proxy
    - Database
    - File
- Major components
  - Data
  - Encryption Engine
  - Keys
    - Internally Managed
    - Externally Managed
    - Escrow Managed

Proxies

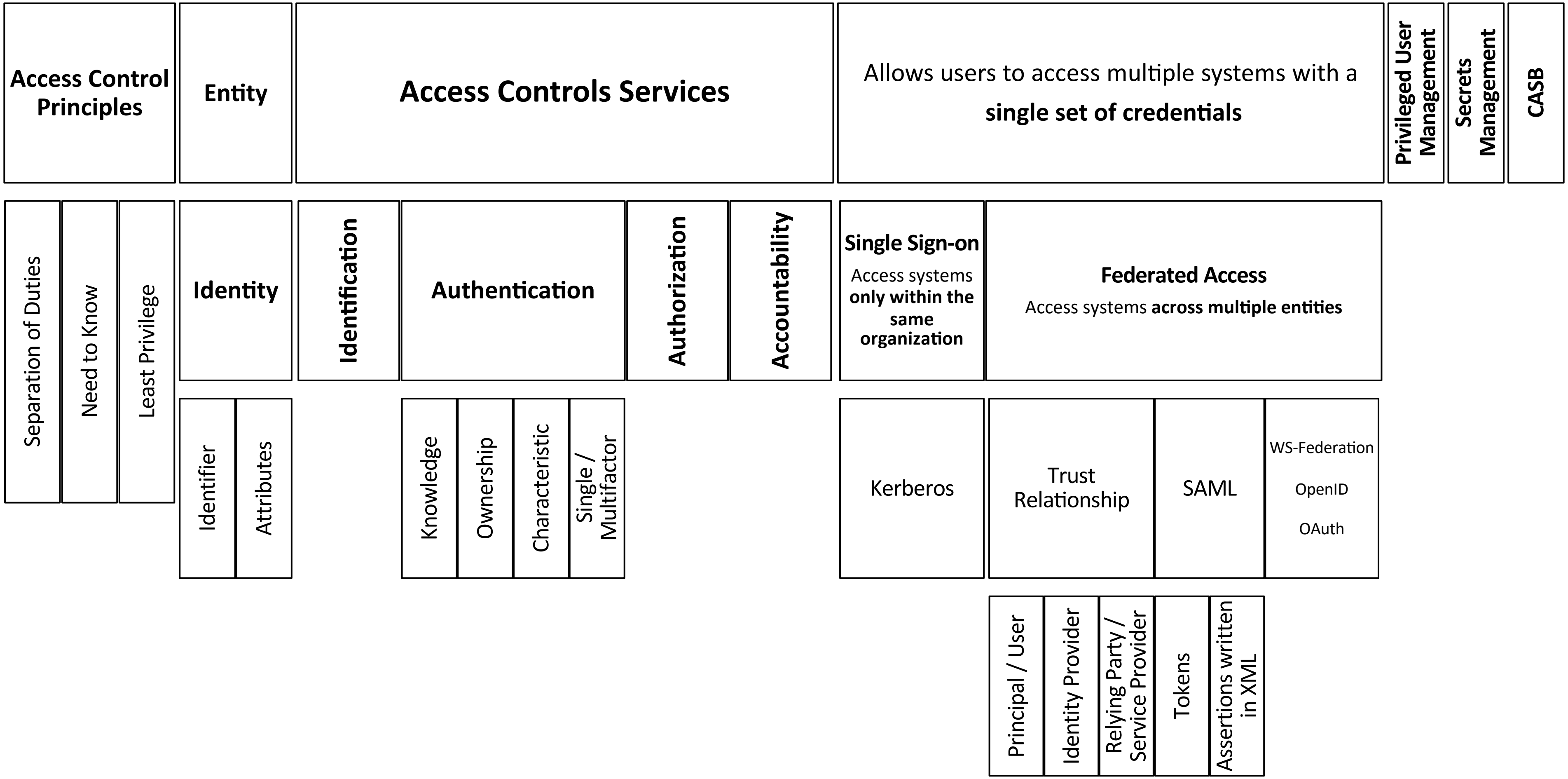
WAF

DAM

FAM

API Gateway

Access Control



Access Control Principles

Separation of Duties

Need to Know

Least Privilege

Entity

Identity

Identifier

Attributes

Access Controls Services

Identification

Authentication

Knowledge

Ownership

Characteristic

Single / Multifactor

Authorization

Accountability

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

Single Sign-on

Access systems **only within the same organization**

Kerberos

Federated Access

Access systems **across multiple entities**

Trust Relationship

Principal / User

Identity Provider

Relying Party / Service Provider

Tokens

Assertions written in XML

SAML

WS-Federation

OpenID

OAuth

Privileged User Management

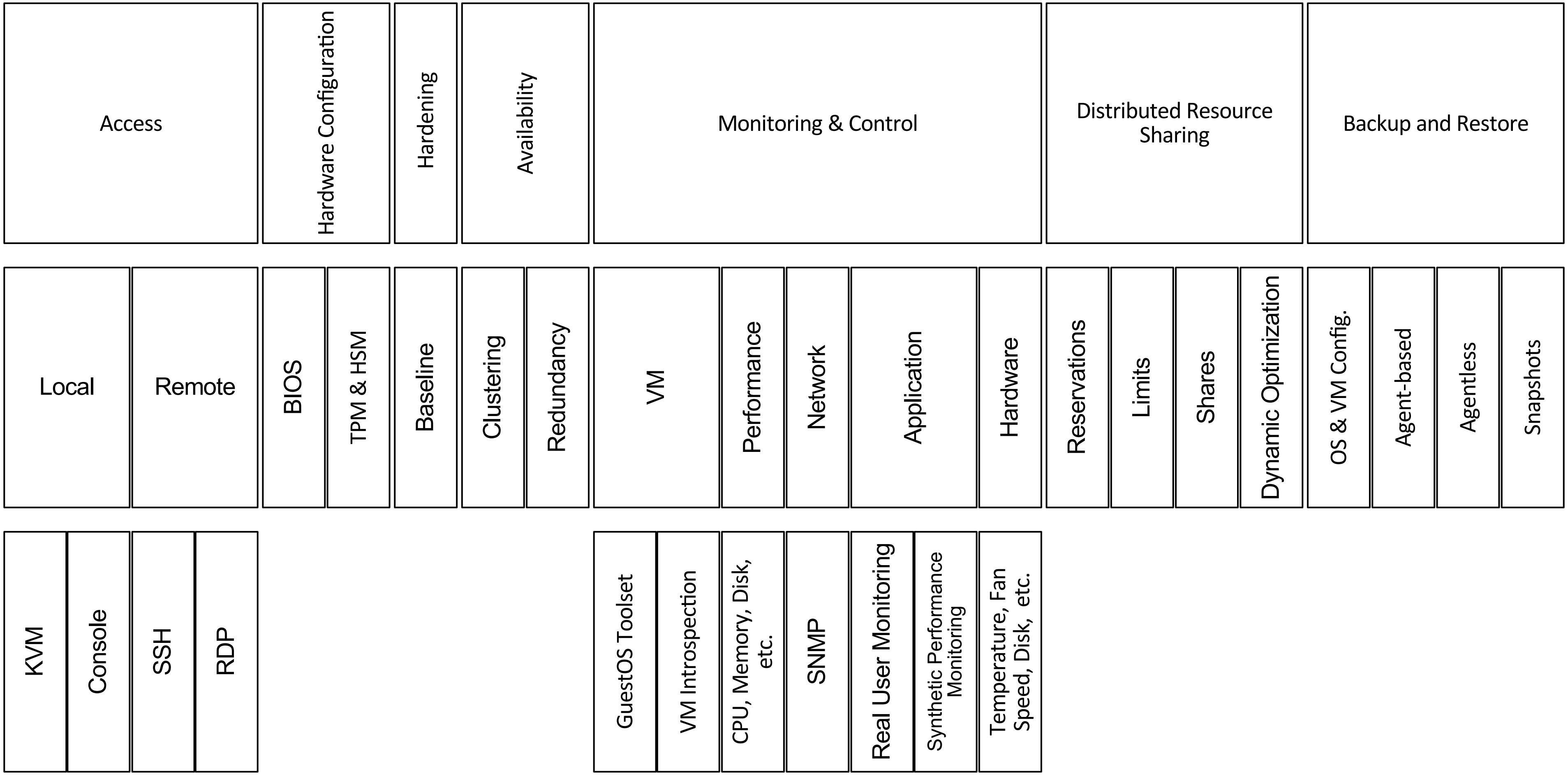
Secrets Management

CASB

5

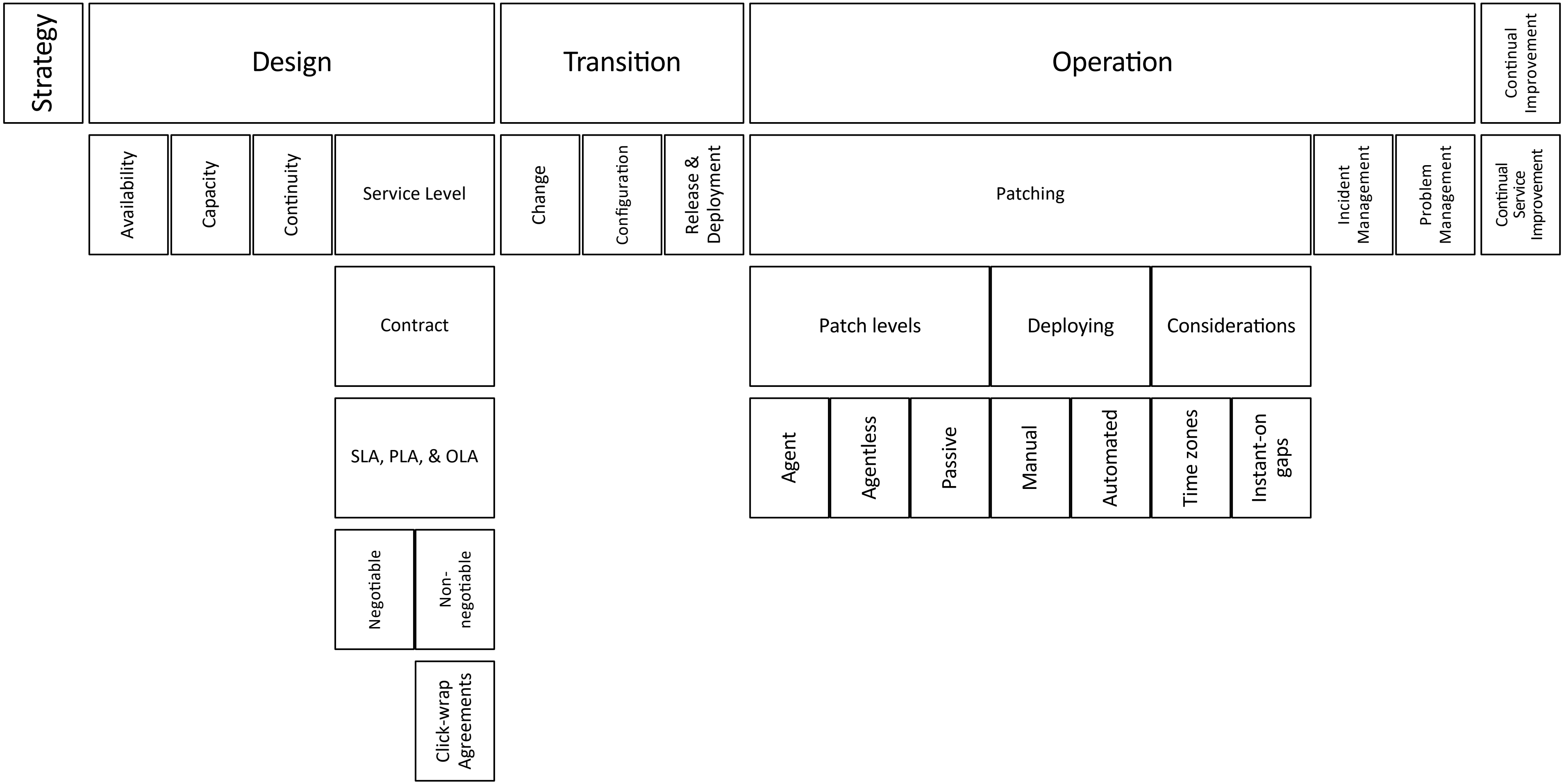
Cloud Security Operations

Cloud Operations



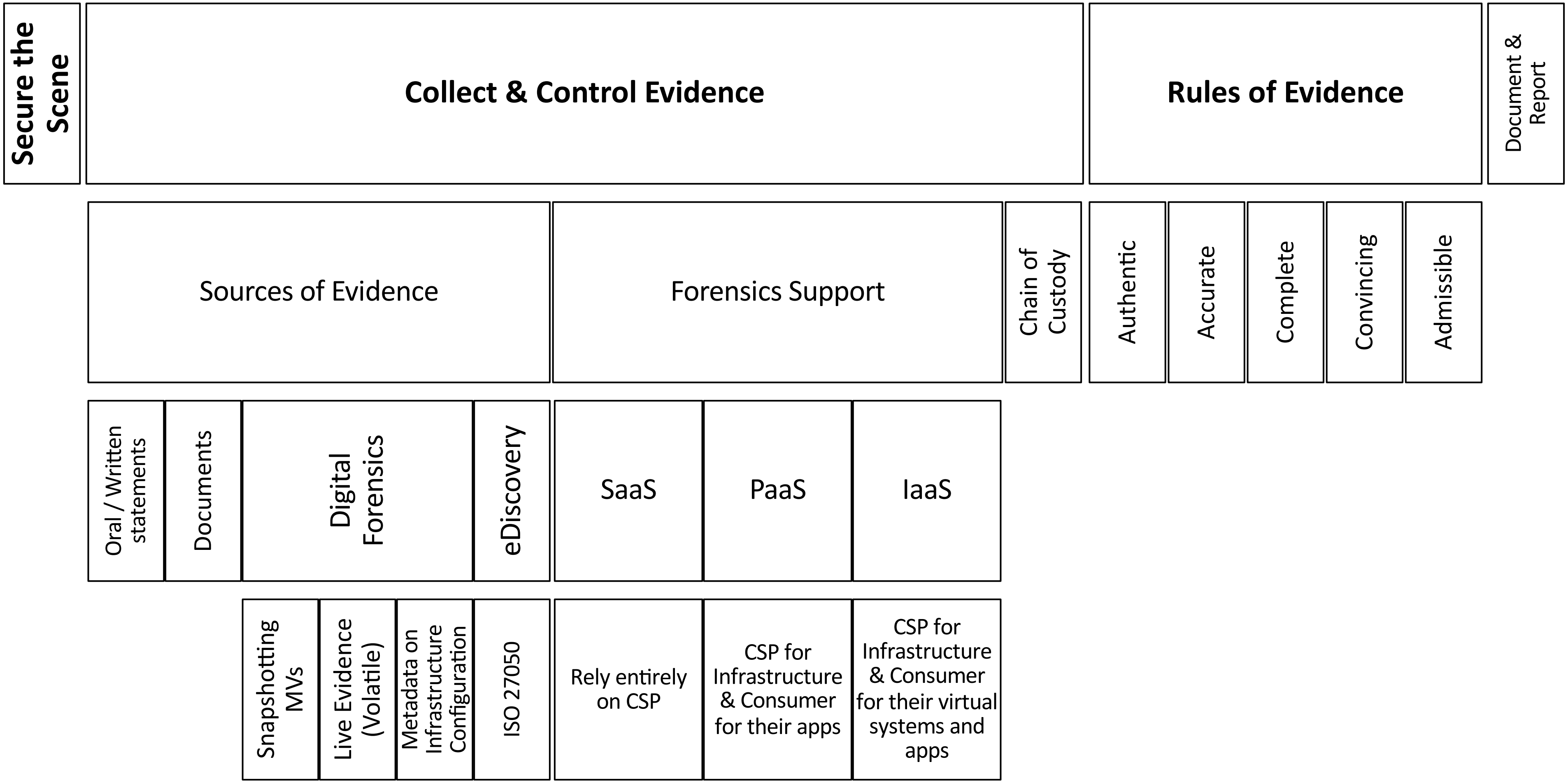
- Access
  - Local
    - KVM
    - Console
  - Remote
    - SSH
    - RDP
- Hardware Configuration
  - BIOS
  - TPM & HSM
- Hardening
  - Baseline
- Availability
  - Clustering
  - Redundancy
- Monitoring & Control
  - VM
    - GuestOS Toolset
    - VM Introspection
  - Performance
    - CPU, Memory, Disk, etc.
  - Network
    - SNMP
  - Application
    - Real User Monitoring
    - Synthetic Performance Monitoring
  - Hardware
    - Temperature, Fan Speed, Disk, etc.
- Distributed Resource Sharing
  - Reservations
  - Limits
  - Shares
  - Dynamic Optimization
- Backup and Restore
  - OS & VM Config.
  - Agent-based
  - Agentless
  - Snapshots

IT Service Management



- Strategy
- Design
  - Availability
  - Capacity
  - Continuity
  - Service Level
    - Contract
      - SLA, PLA, & OLA
        - Negotiable
        - Non-negotiable
          - Click-wrap Agreements
- Transition
  - Change
  - Configuration
  - Release & Deployment
- Operation
  - Patching
    - Patch levels
      - Agent
      - Agentless
      - Passive
    - Deploying
      - Manual
      - Automated
    - Considerations
      - Time zones
      - Instant-on gaps
  - Incident Management
  - Problem Management
- Continual Improvement
  - Continual Service Improvement

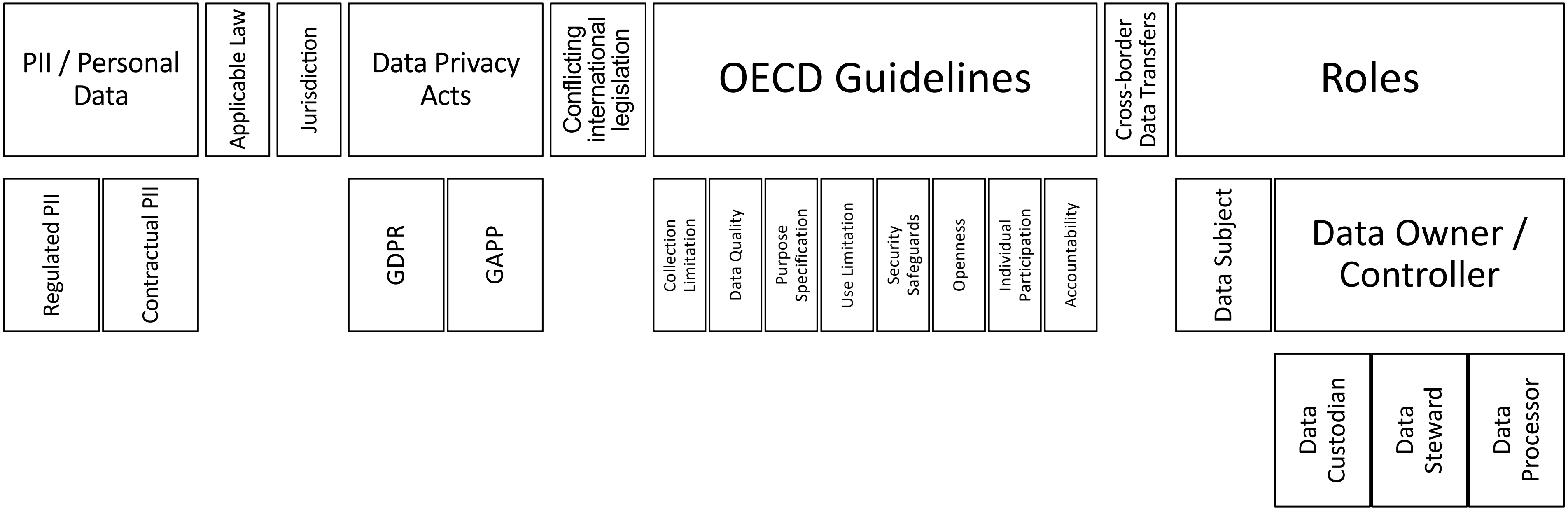
Investigations



6

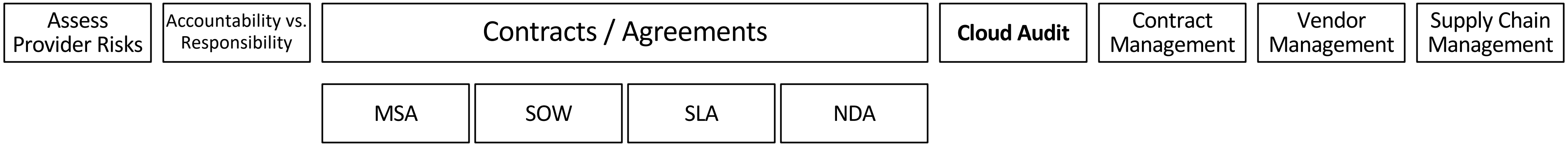
Legal, Risk and Compliance

Privacy



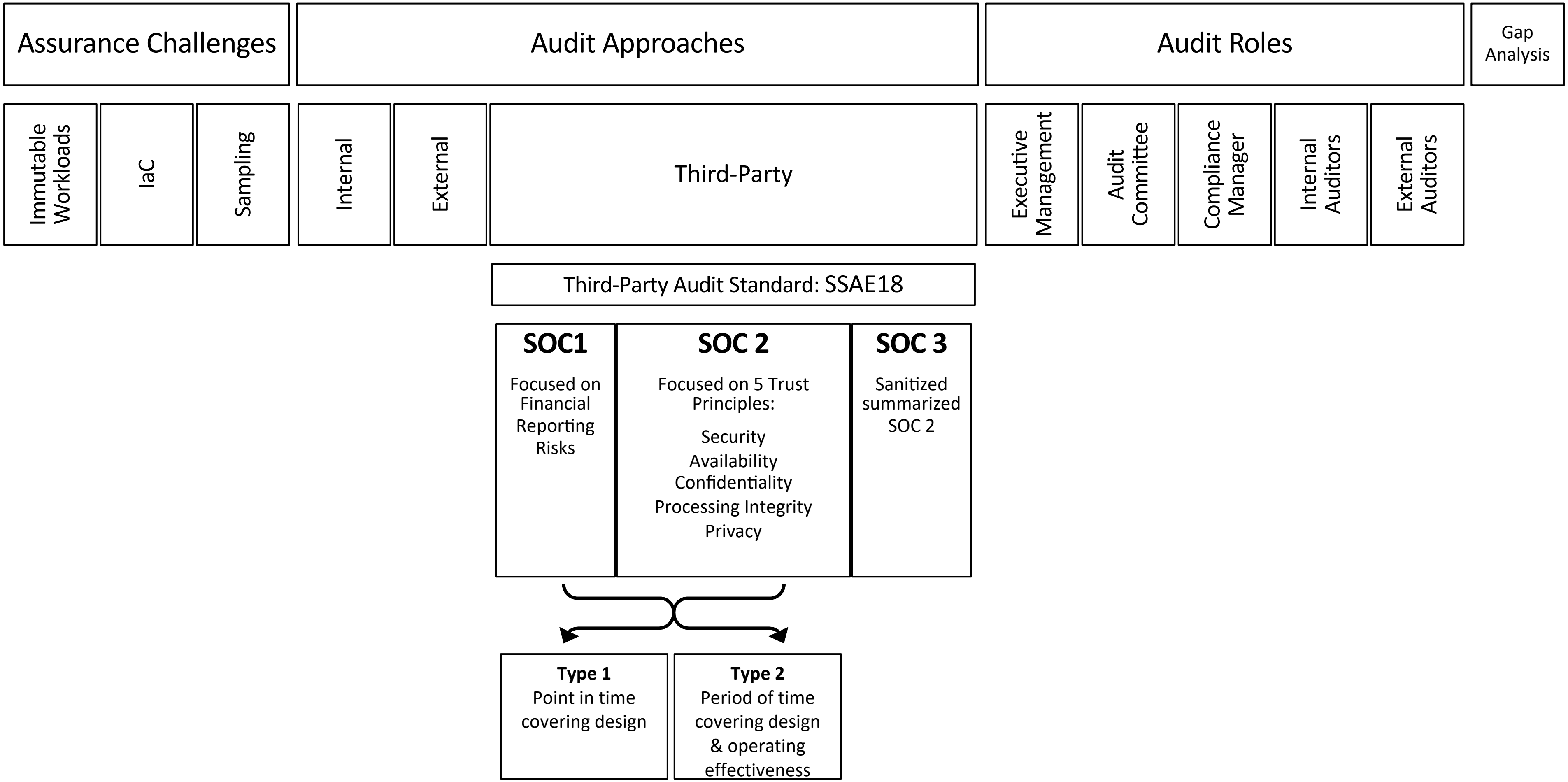
- PII / Personal Data
  - Regulated PII
  - Contractual PII
- Applicable Law
- Jurisdiction
- Data Privacy Acts
  - GDPR
  - GAPP
- Conflicting international legislation
- OECD Guidelines
  - Collection Limitation
  - Data Quality
  - Purpose Specification
  - Use Limitation
  - Security Safeguards
  - Openness
  - Individual Participation
  - Accountability
- Cross-border Data Transfers
- Roles
  - Data Subject
  - Data Owner / Controller
    - Data Custodian
    - Data Steward
    - Data Processor

Outsourcing & Cloud Contracts



- Assess Provider Risks
- Accountability vs. Responsibility
- Contracts / Agreements
  - MSA
  - SOW
  - SLA
  - NDA
- **Cloud Audit**
- Contract Management
- Vendor Management
- Supply Chain Management

Cloud Audit



Assurance Challenges

Immutable Workloads

IaC

Sampling

Audit Approaches

Internal

External

Third-Party

Third-Party Audit Standard: SSAE18

SOC1

Focused on Financial Reporting Risks

SOC 2

Focused on 5 Trust Principles:

Security
Availability
Confidentiality
Processing Integrity
Privacy

SOC 3

Sanitized summarized SOC 2

Type 1
Point in time covering design

Type 2
Period of time covering design & operating effectiveness

Audit Roles

Executive Management

Audit Committee

Compliance Manager

Internal Auditors

External Auditors

Gap Analysis

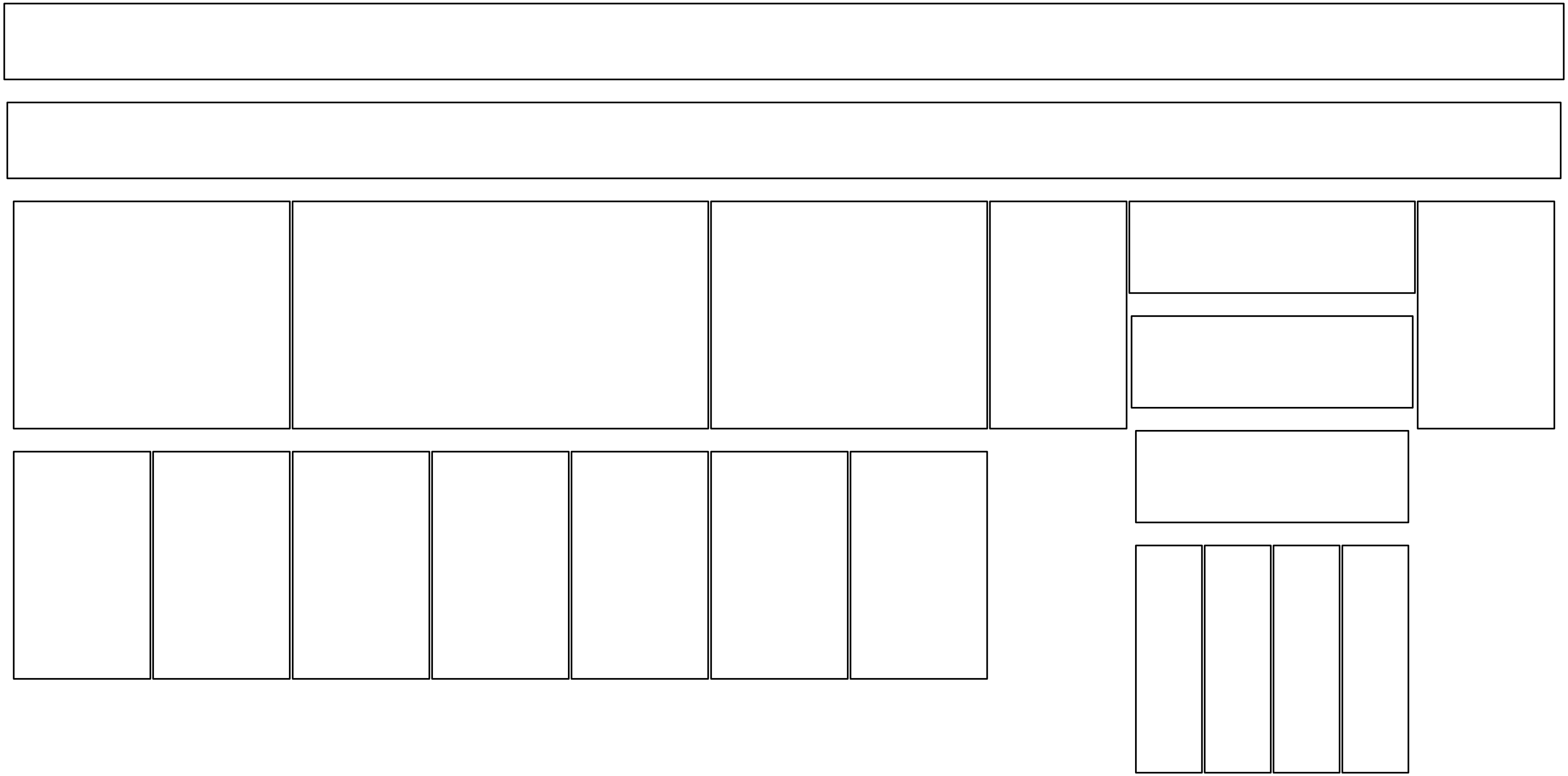
Printable Blank CCSP MindMaps

Print out the following blank MindMaps and fill them in as your watch our MindMap videos!

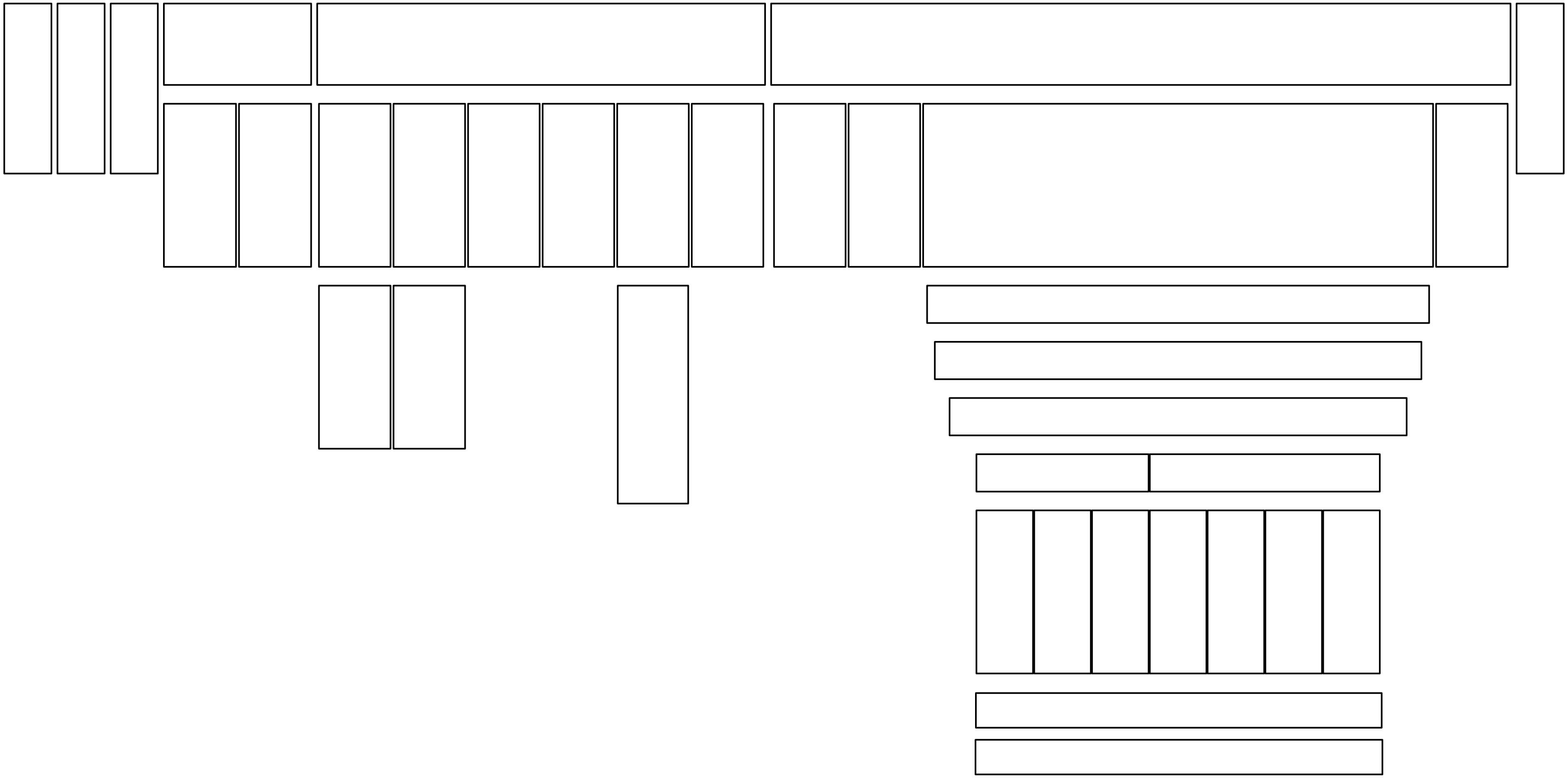
Print pages **38** to **66**

Cloud Computing

Alignment of Security Function to Business Strategy



Risk Management



Cloud Shared Considerations

Frameworks

Cost Benefit Analysis

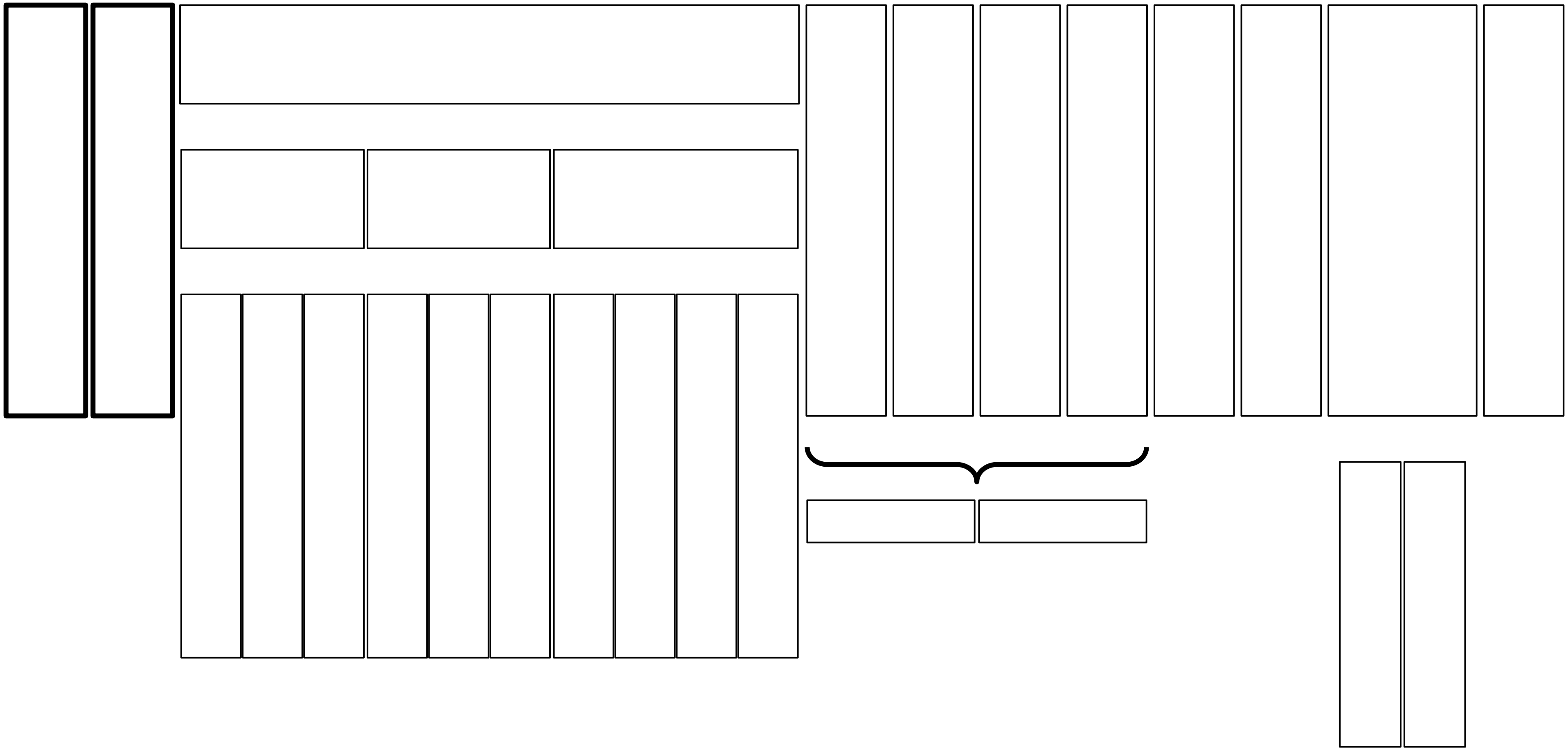
Evaluation Criteria

Cloud Data Lifecycle

Cloud Data Storage

Threats to Storage

Data Security Strategies



Data Discovery

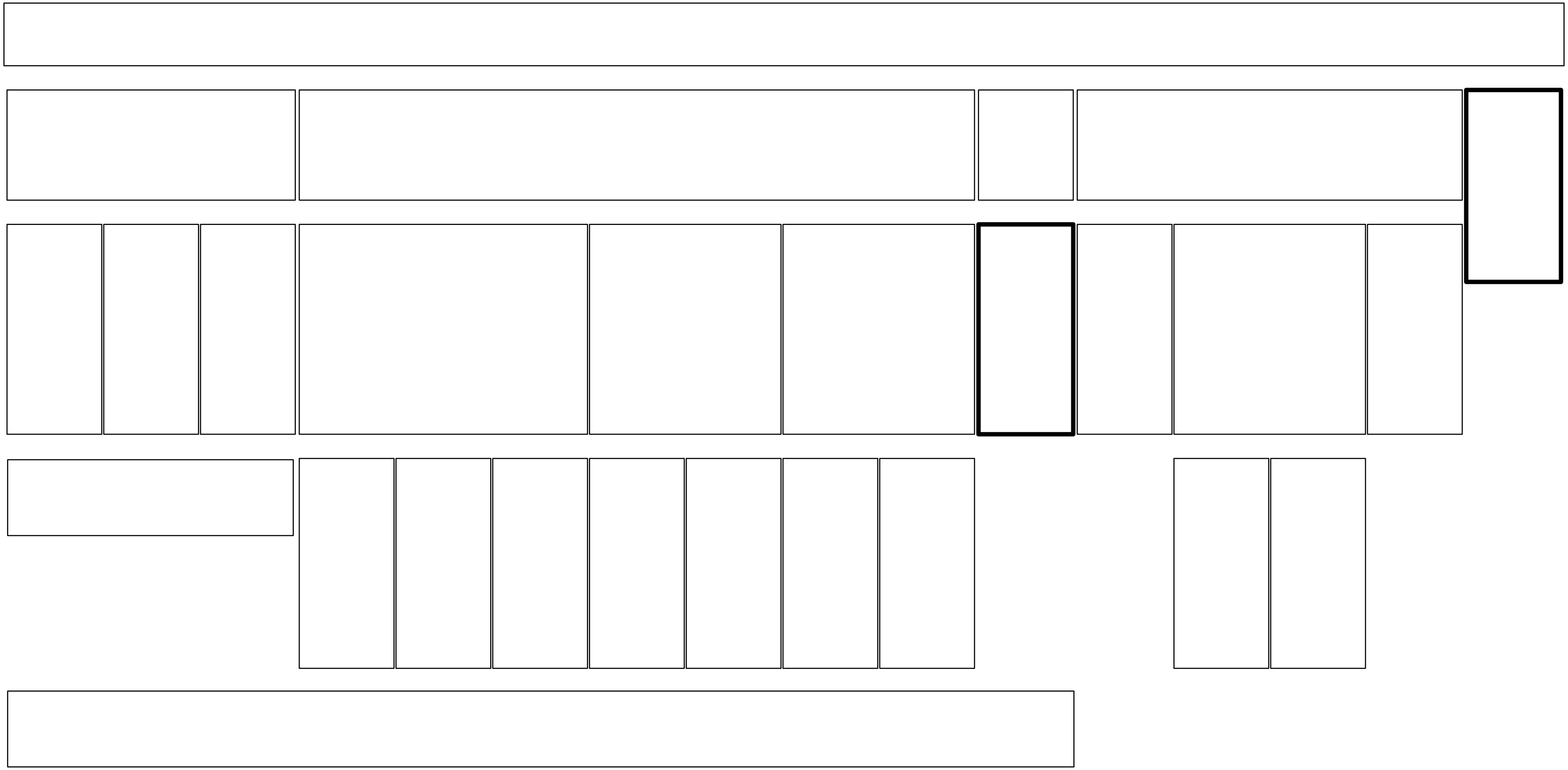
Asset Classification

Log Review & Analysis

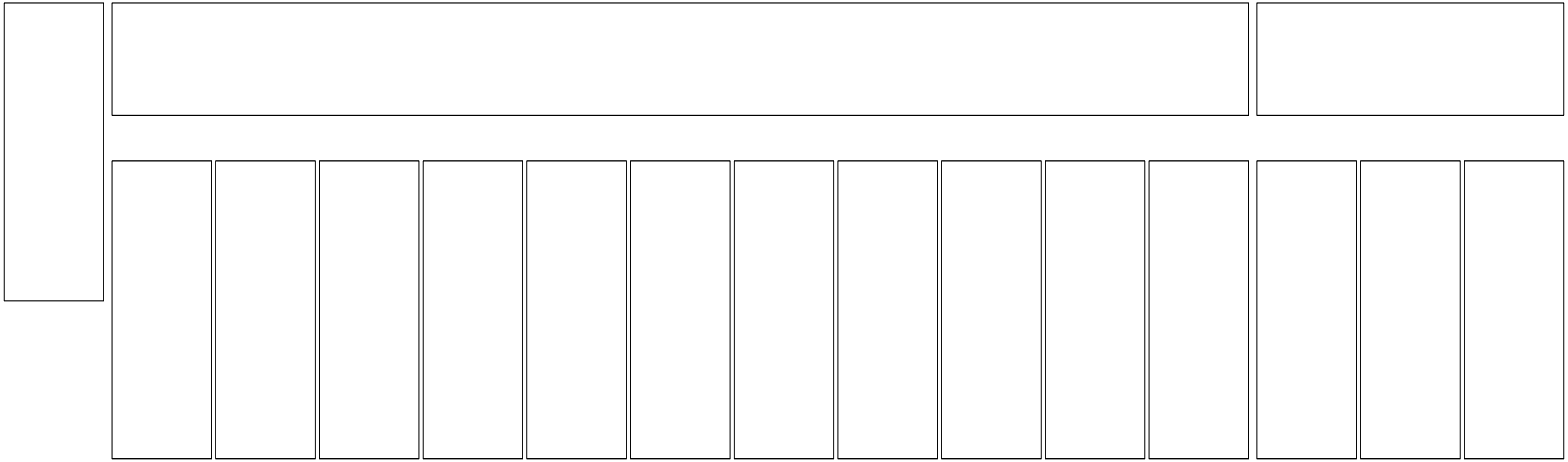
Digital Rights Management (DRM)

Data Retention, Archiving & Deletion

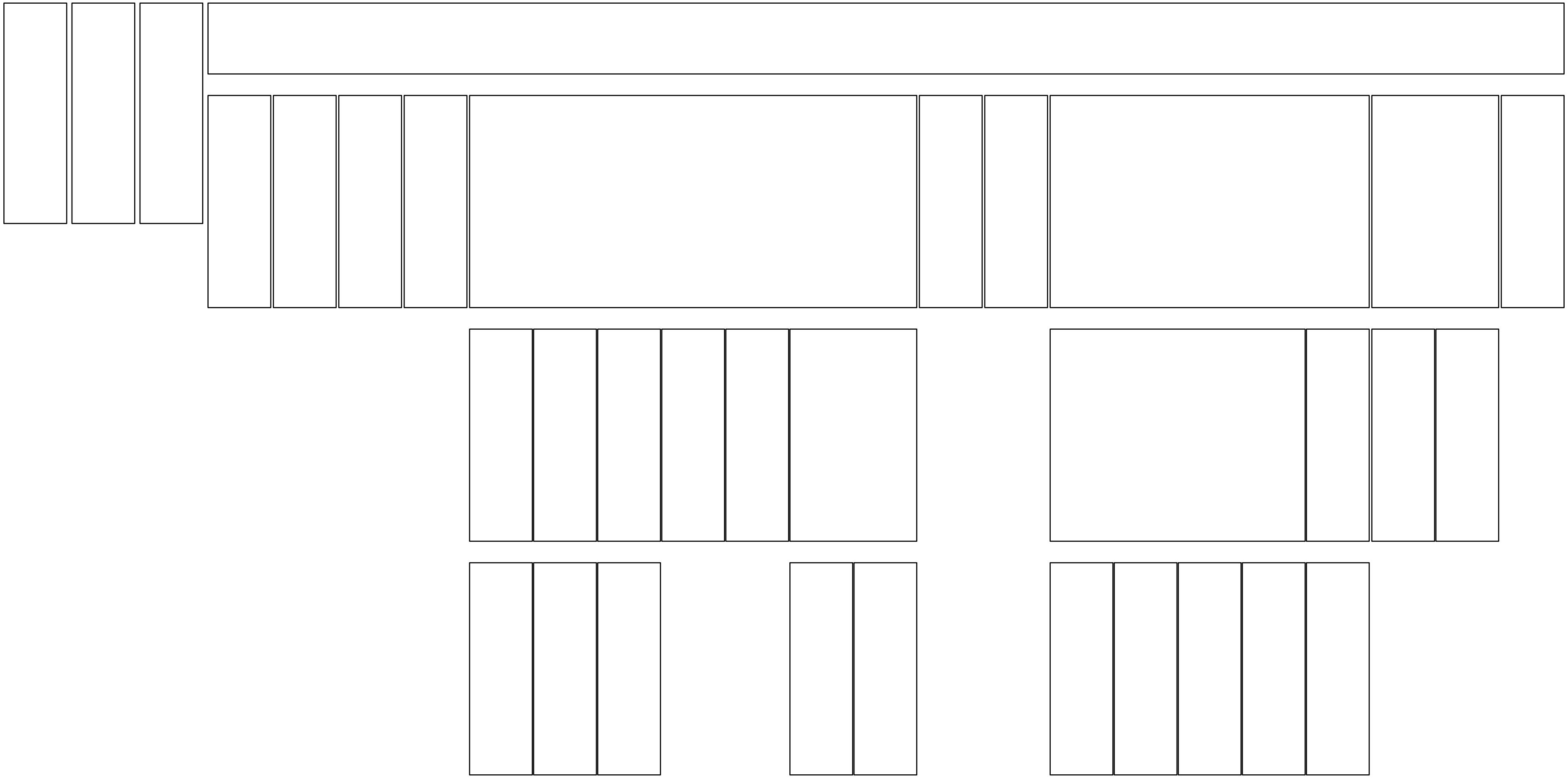
Cloud Infrastructure Components



Management Plane



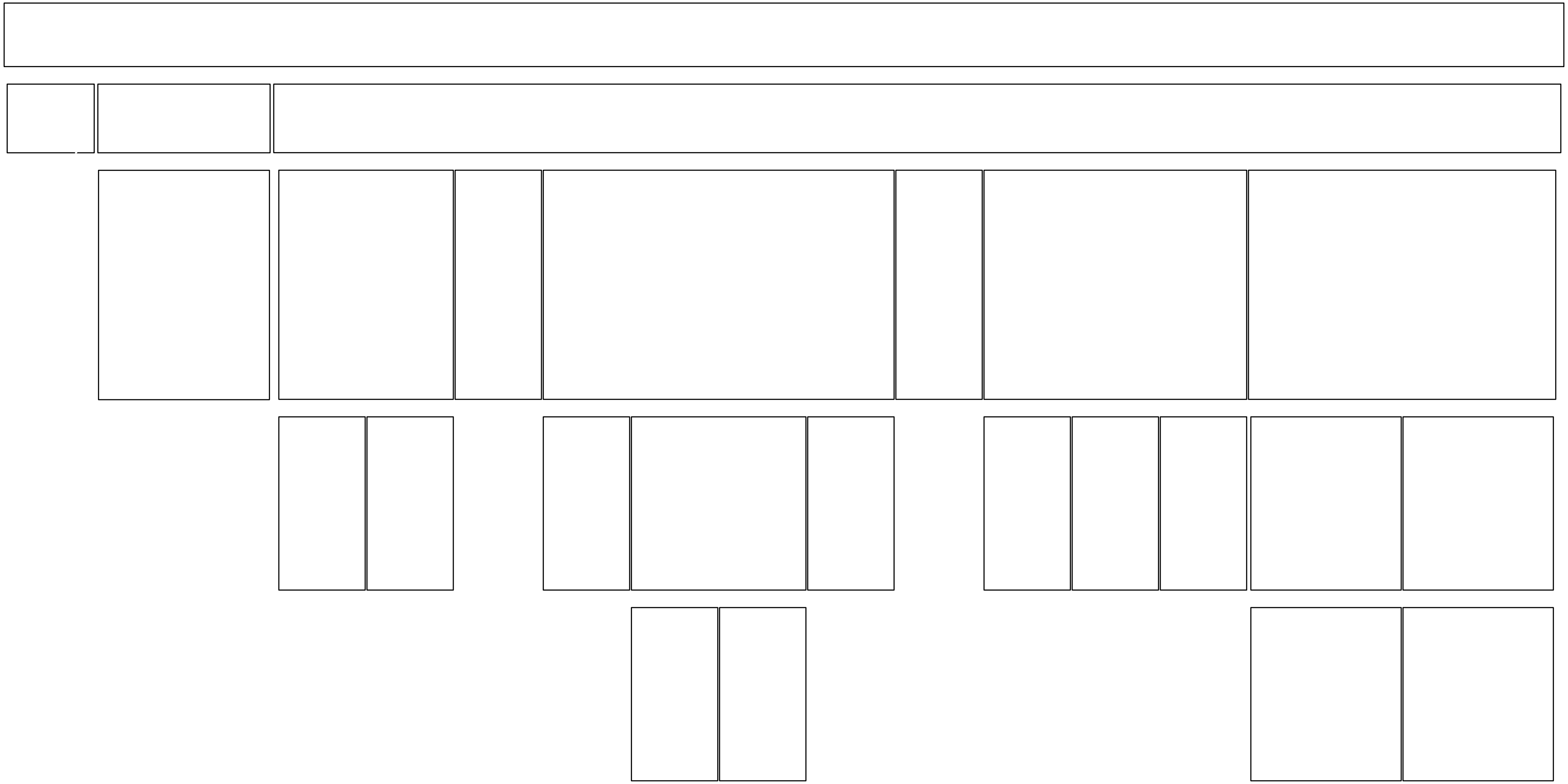
Data Center Design



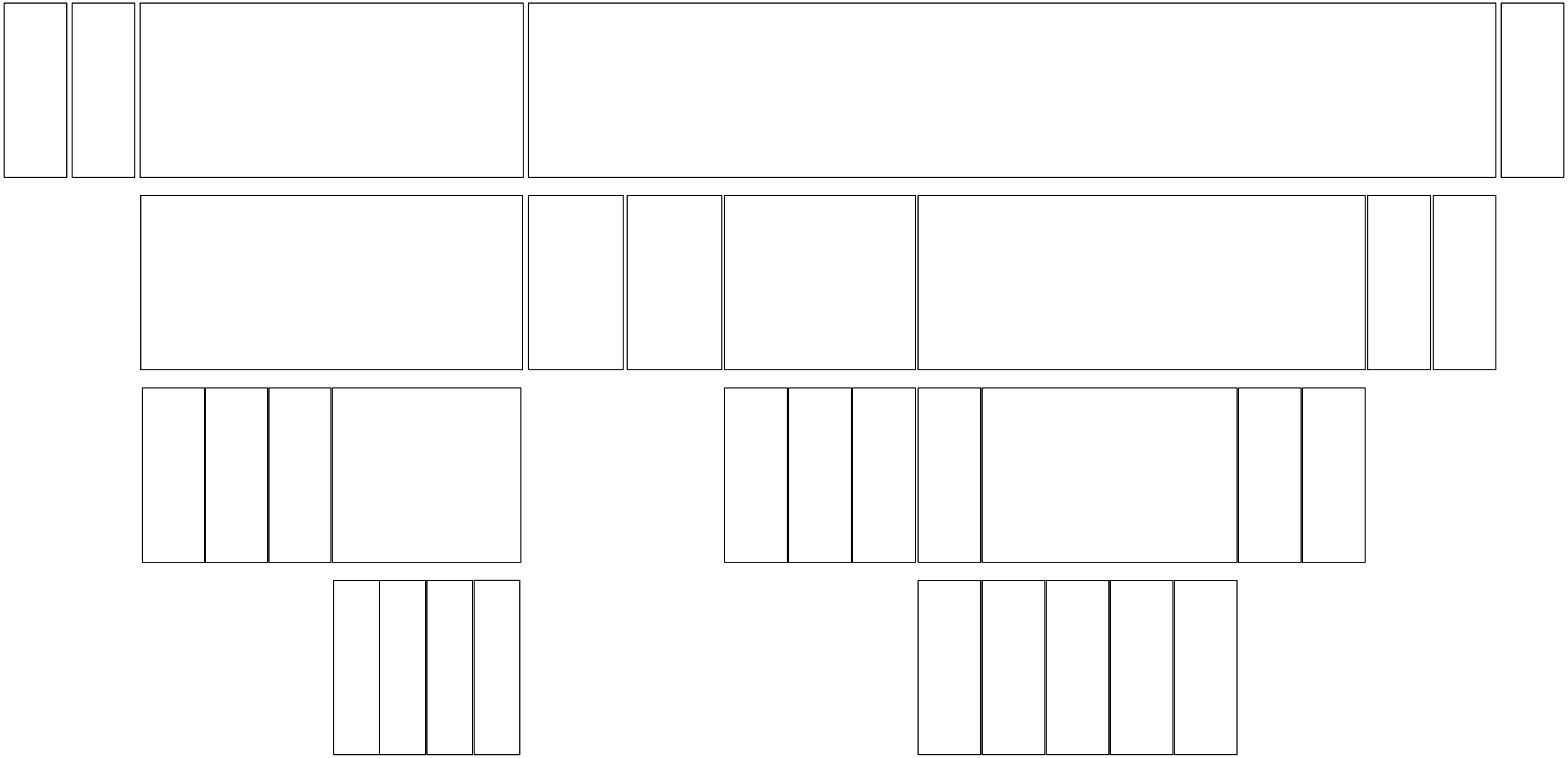
Attack Vectors

Risks

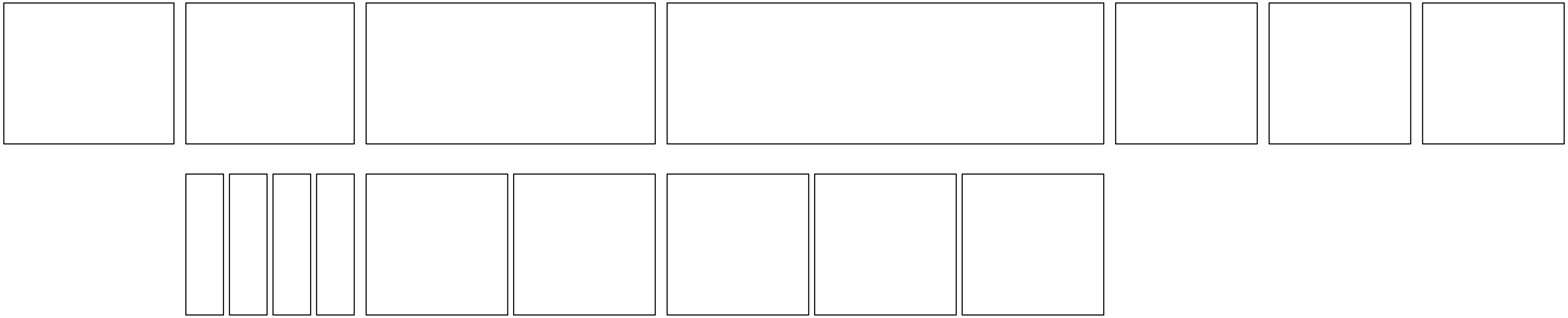
Physical Security



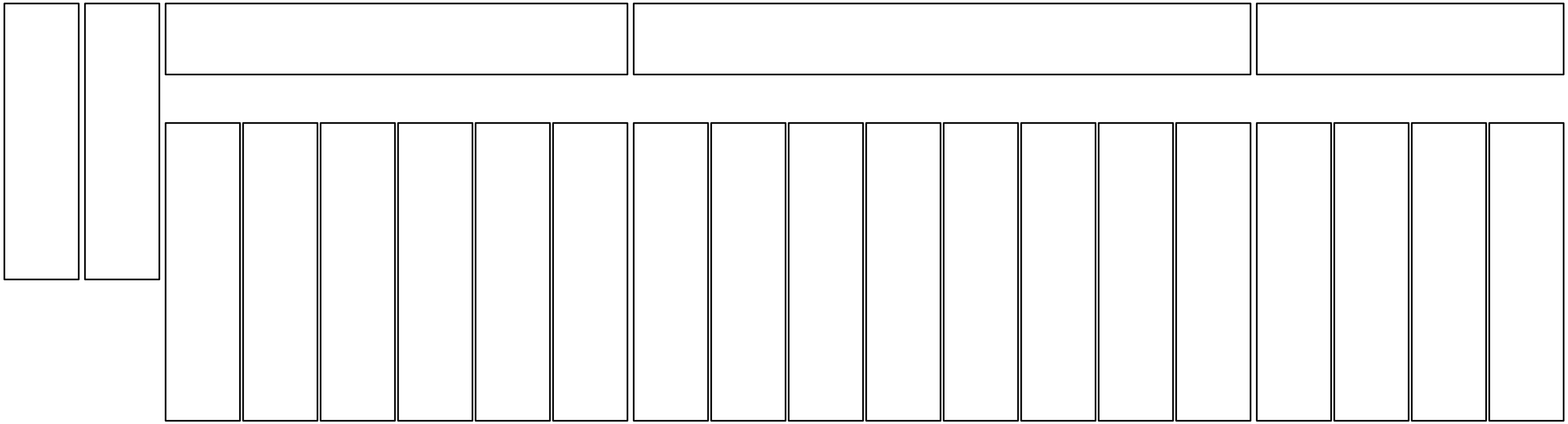
Network Defense



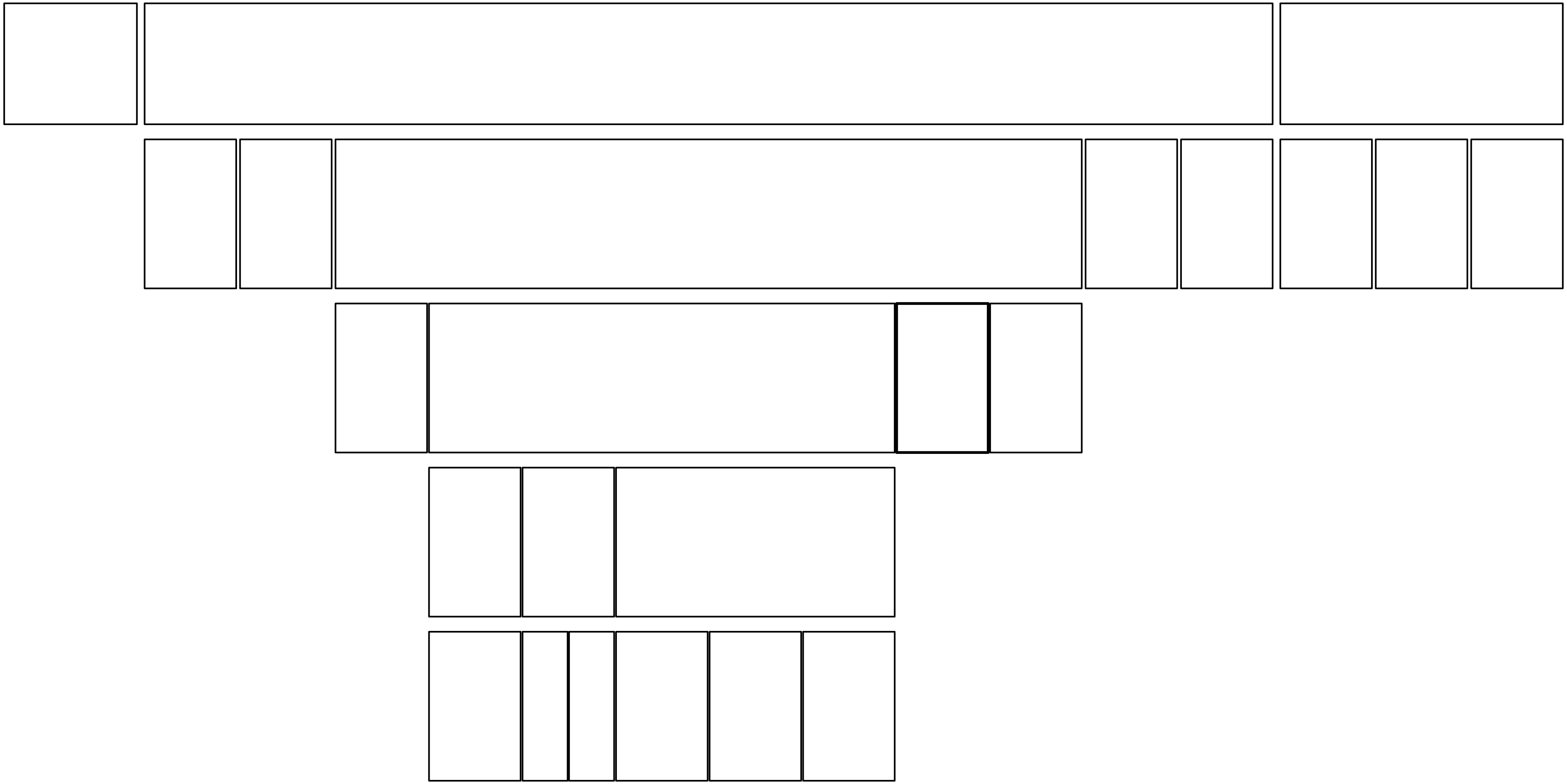
Business Continuity Management (BCM)



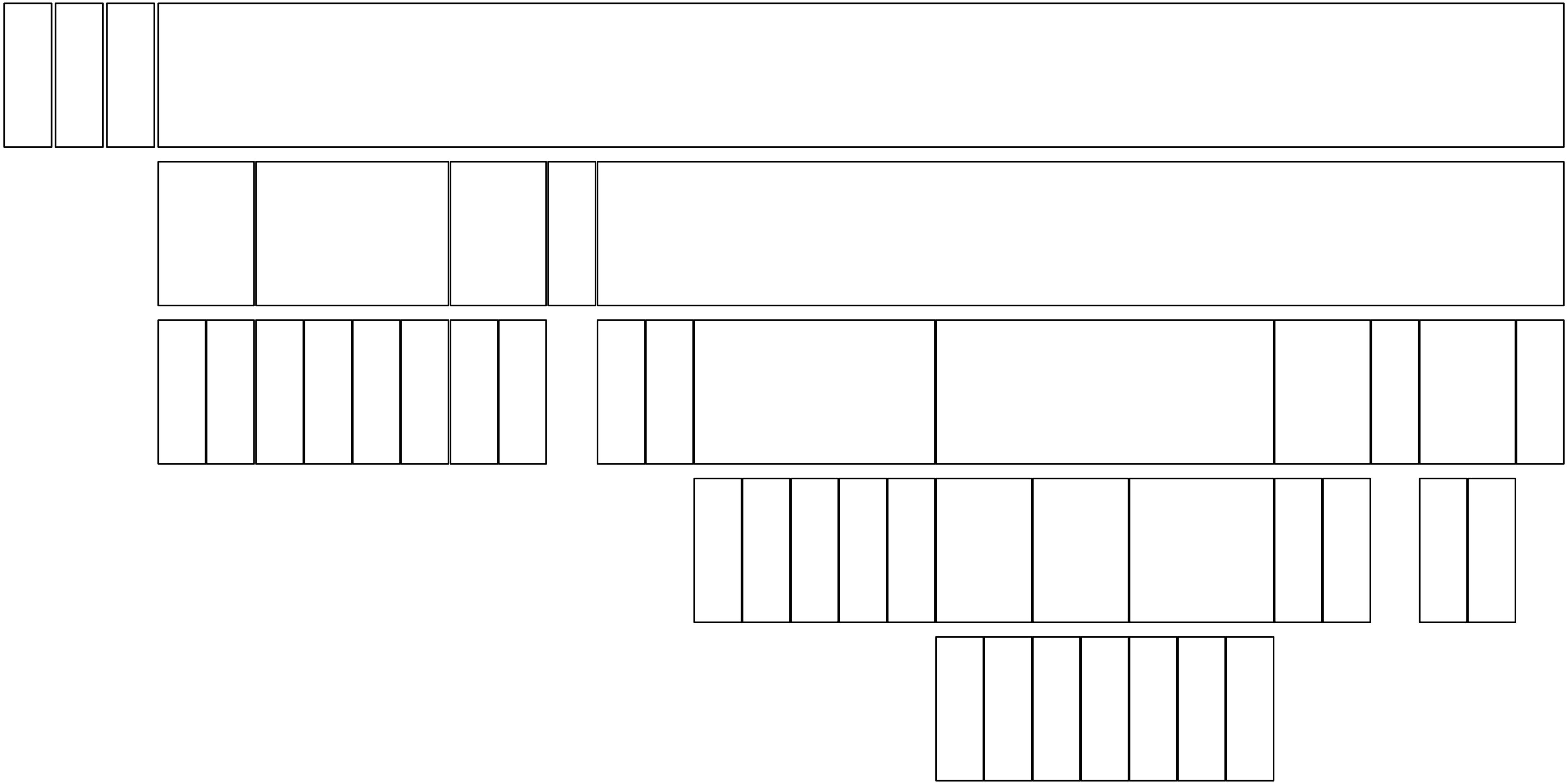
Cloud Development



Secure Software Development



Security Assessment and Testing



Common Vulnerabilities & Threat Modeling

Verified Secure Software

Cryptographic Services

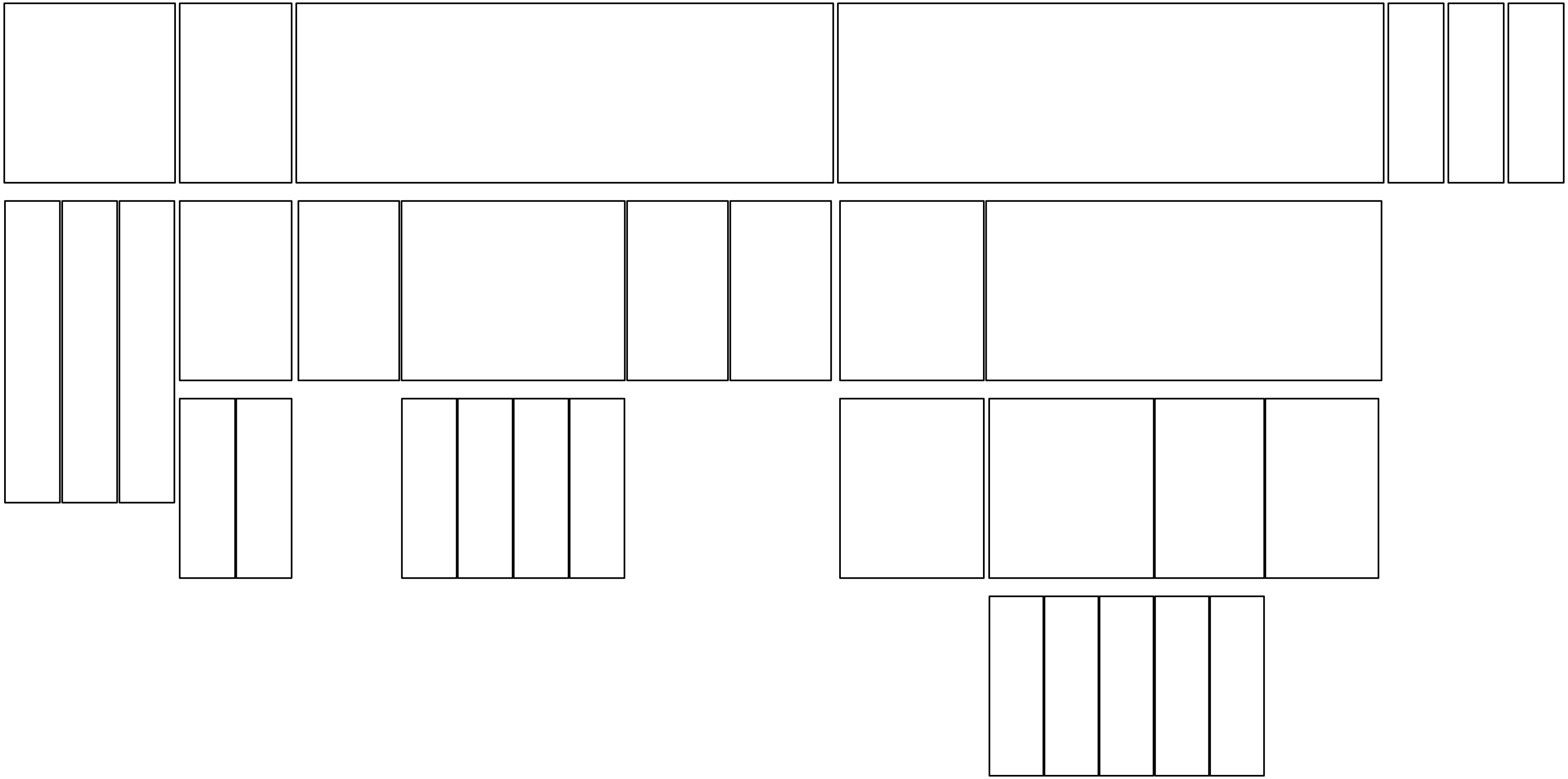
Cryptography

Key Management

Crypto in the Clouds

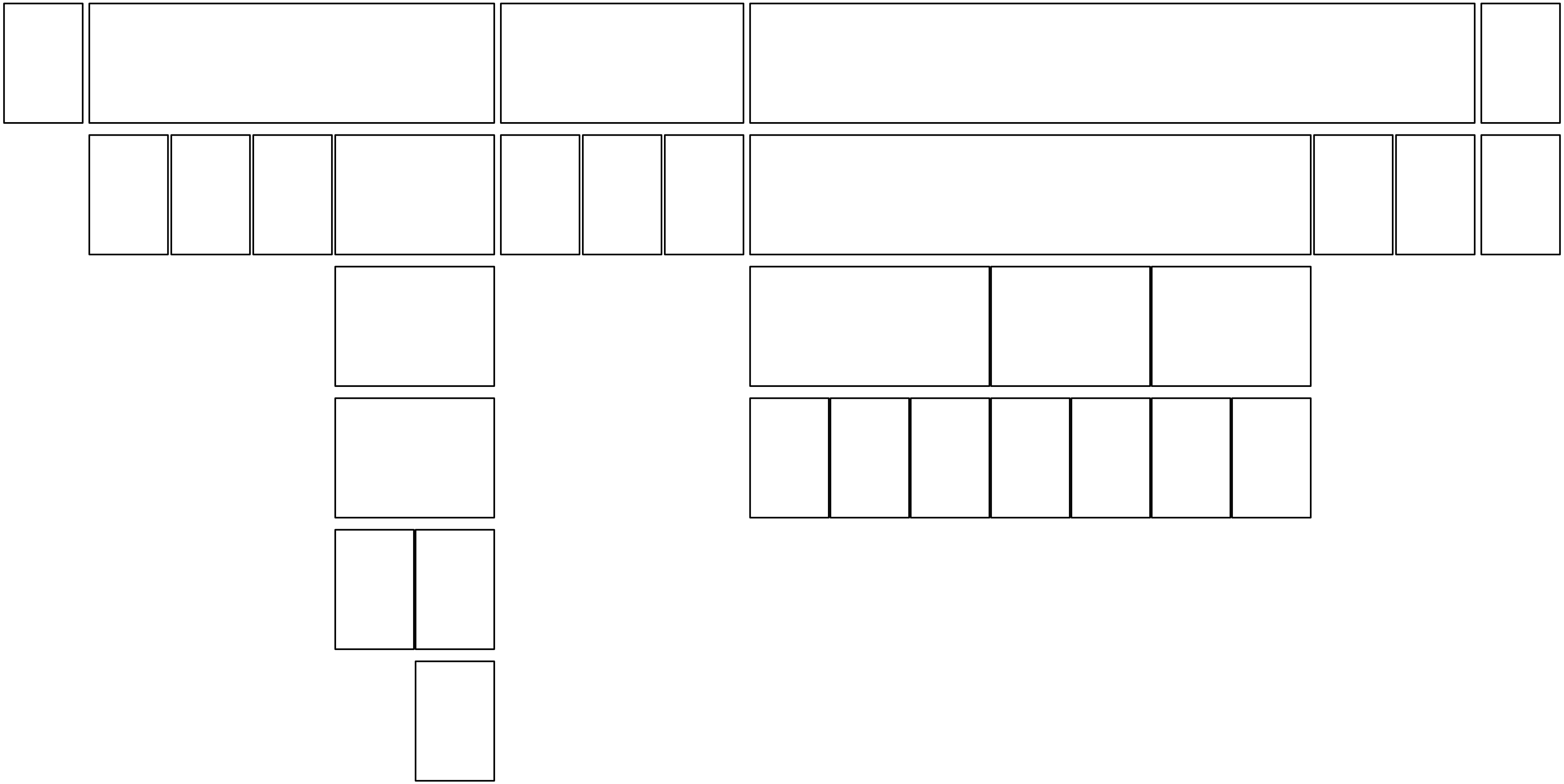
Proxies

Access Control



Cloud Operations

IT Service Management



Investigations

Privacy

Outsourcing & Cloud Contracts

Cloud Audit