CCSP
MindMaps

Domain 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

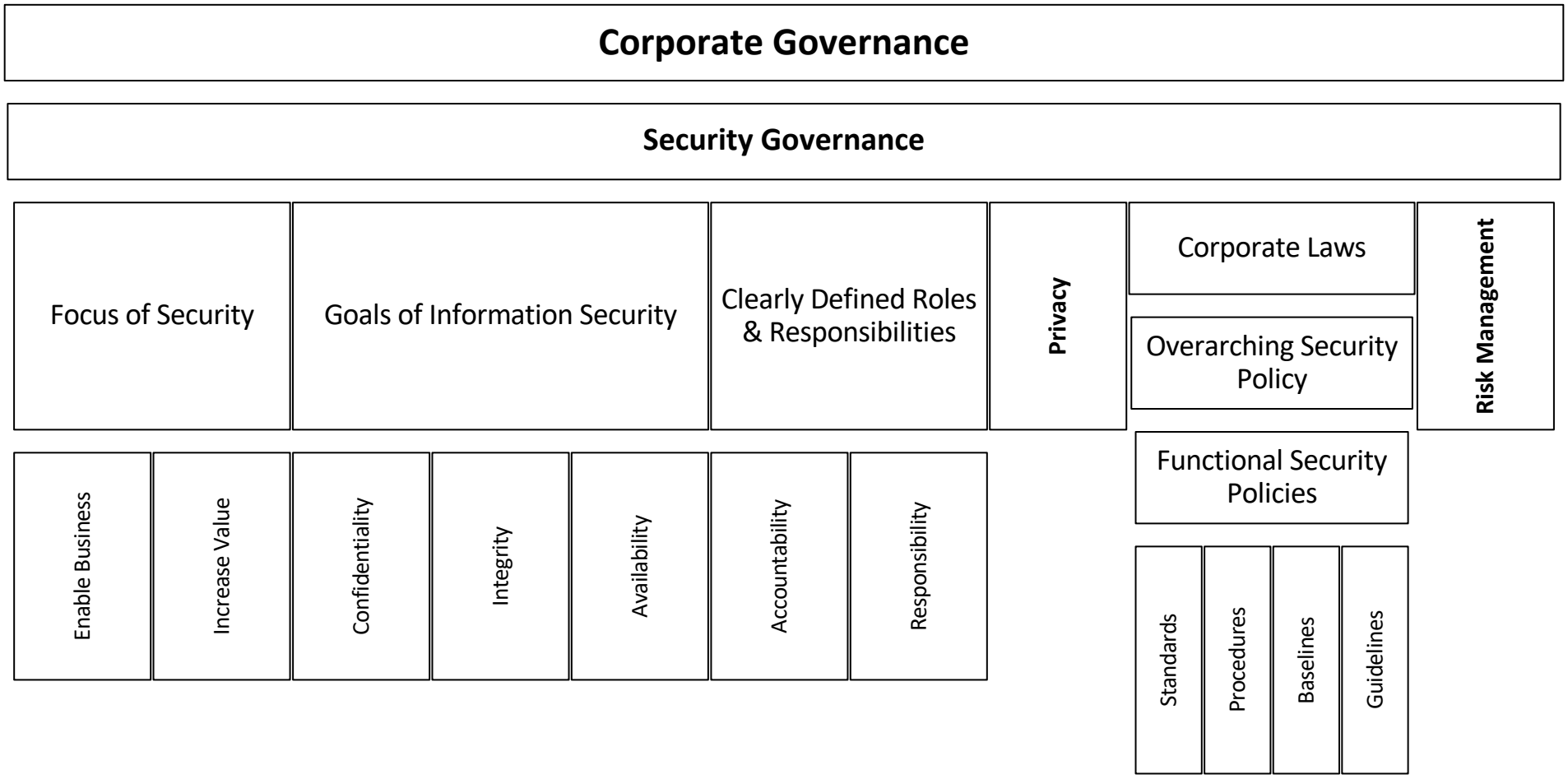
Service Models

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

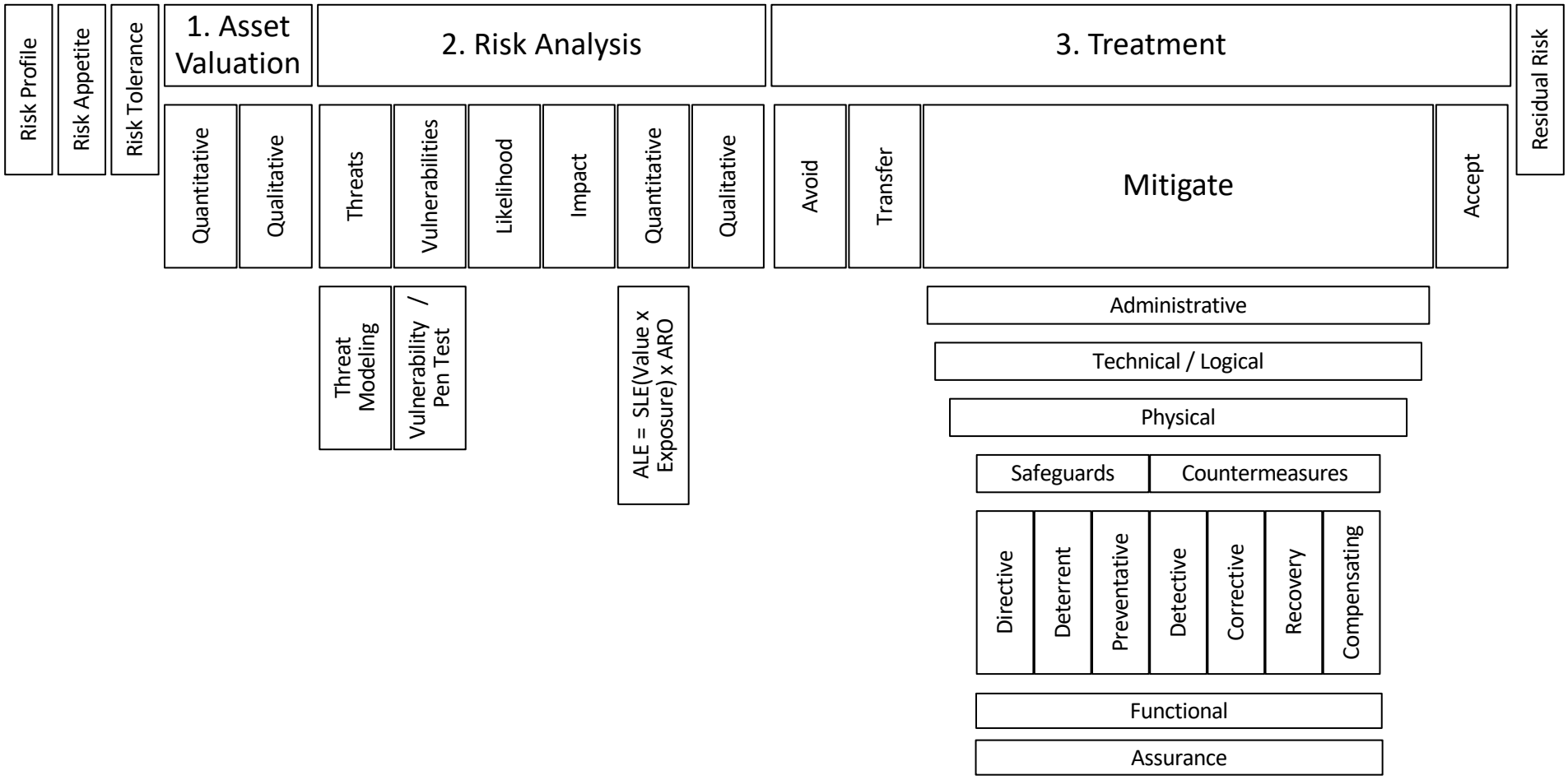
Deployment Models

- Public
- Private
- Community
- Hybrid
- Multi

Alignment of Security Function to Business Strategy



Risk Management



Cloud Shared Considerations

Cloud must be a business decision

Interoperability	**Data** Portability	Application Portability	Reversibility	Availability	Security	Privacy	Resiliency	Performance	Governance	Service Level Agreements (SLA**s**)	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

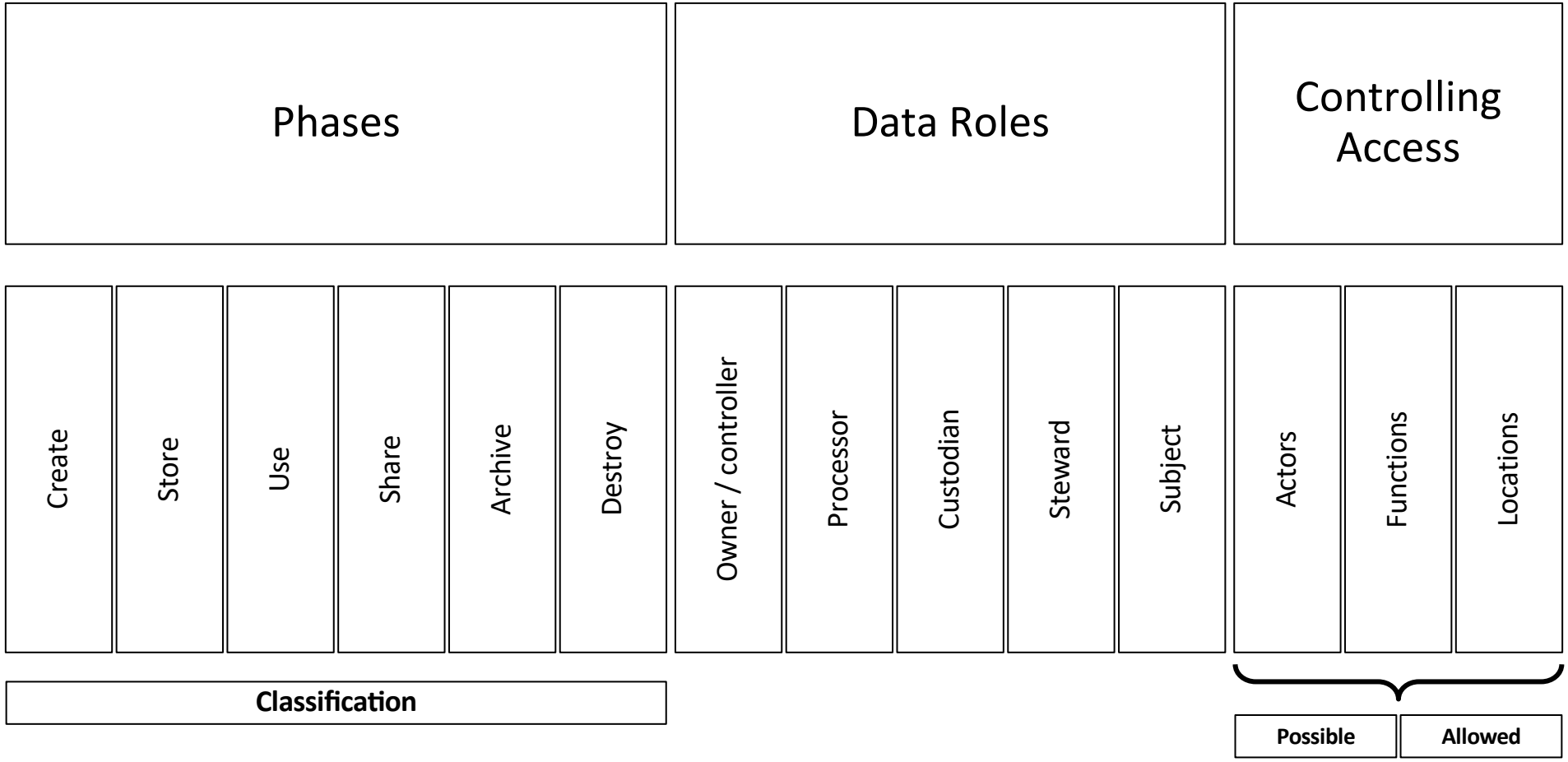
Common Criteria	**FIPS 140-2**
EAL1 – EAL7	**Levels 1 - 4**

Accreditation

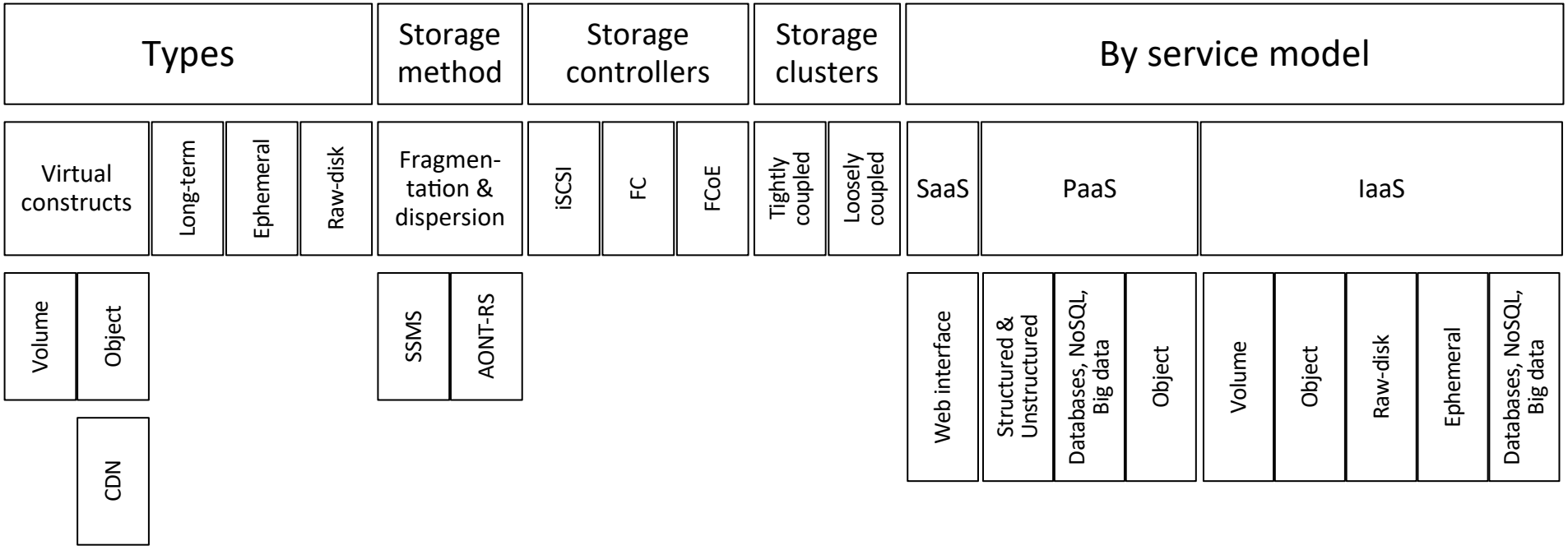
Domain 2

Cloud Data Security

Cloud Data Lifecycle



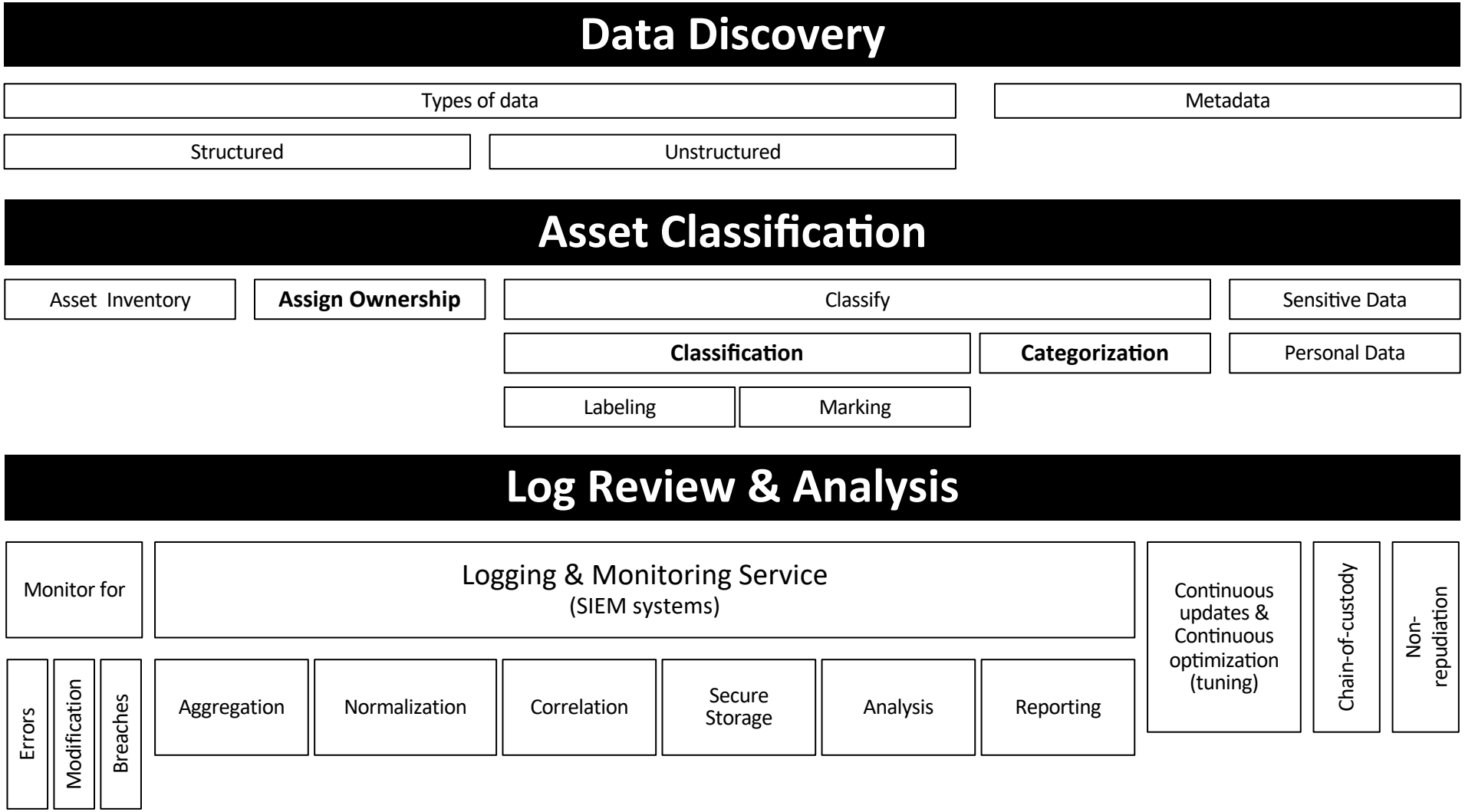
Cloud Data Storage



Threats to Storage

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

Data Security Strategies


Data Discovery
Types of data
Metadata
Structured
Unstructured
Asset Classification
Asset Inventory
Assign Ownership
Classify
Sensitive Data
Classification
Categorization
Personal Data
Labeling
Marking
Log Review & Analysis
Monitor for
Logging & Monitoring Service
(SIEM systems)
Continuous updates & Continuous optimization (tuning)
Chain-of-custody
Non-repudiation
Errors
Modification
Breaches
Aggregation
Normalization
Correlation
Secure Storage
Analysis
Reporting

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

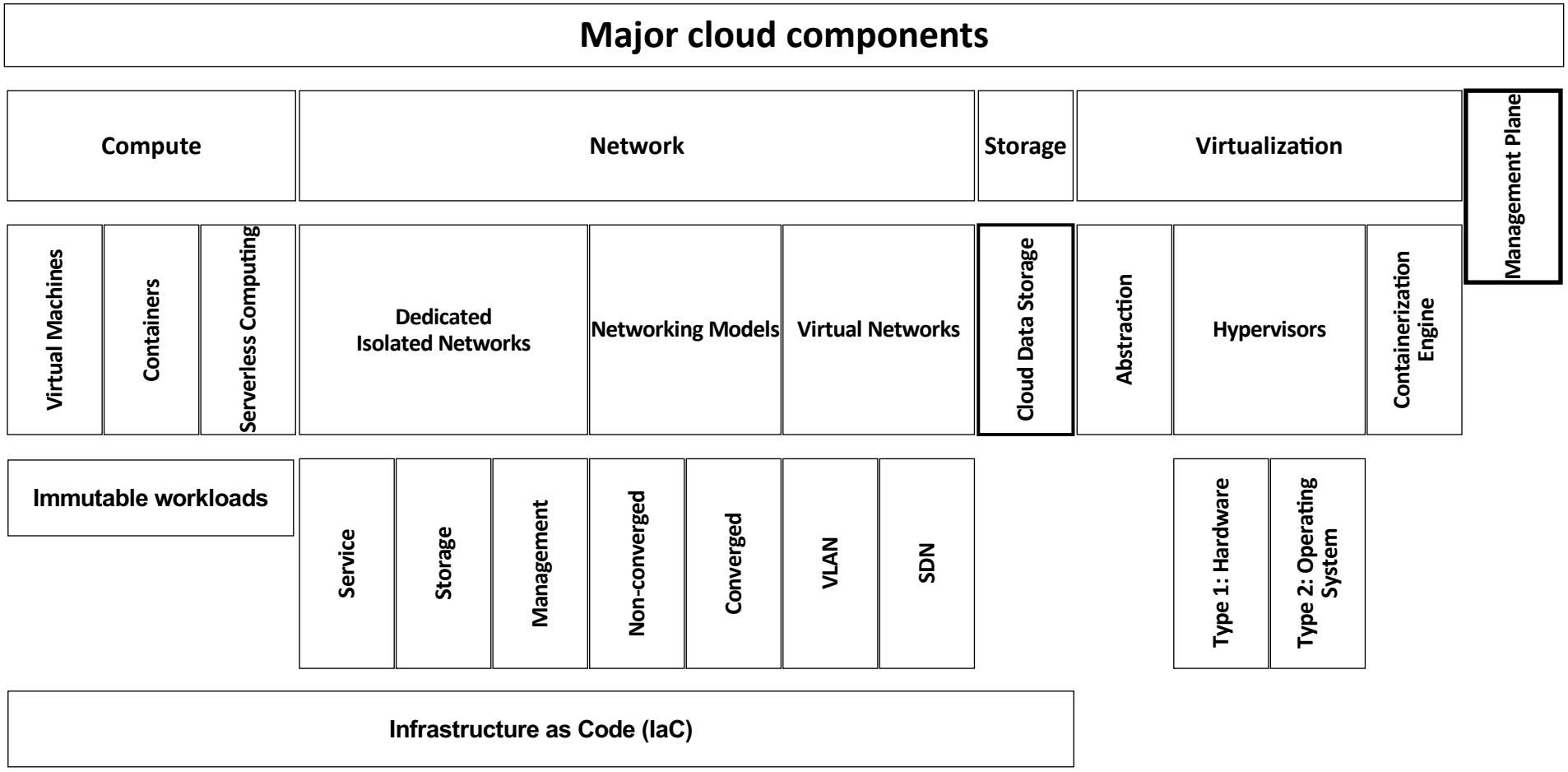
Data Retention, Archiving & Deletion

- Data retention policies
- Migration to slower storage
- Defensible Destruction
  - Destruction
    - Media Destruction
    - Shred / Disintegrate / Drill
    - Degauss
  - Purging
    - Crypto shredding
  - Clearing
    - Overwrite / Wipe / Erasure
    - Format

Domain 3

Cloud Platform and Infrastructure Security

Cloud Infrastructure Components



Management Plane

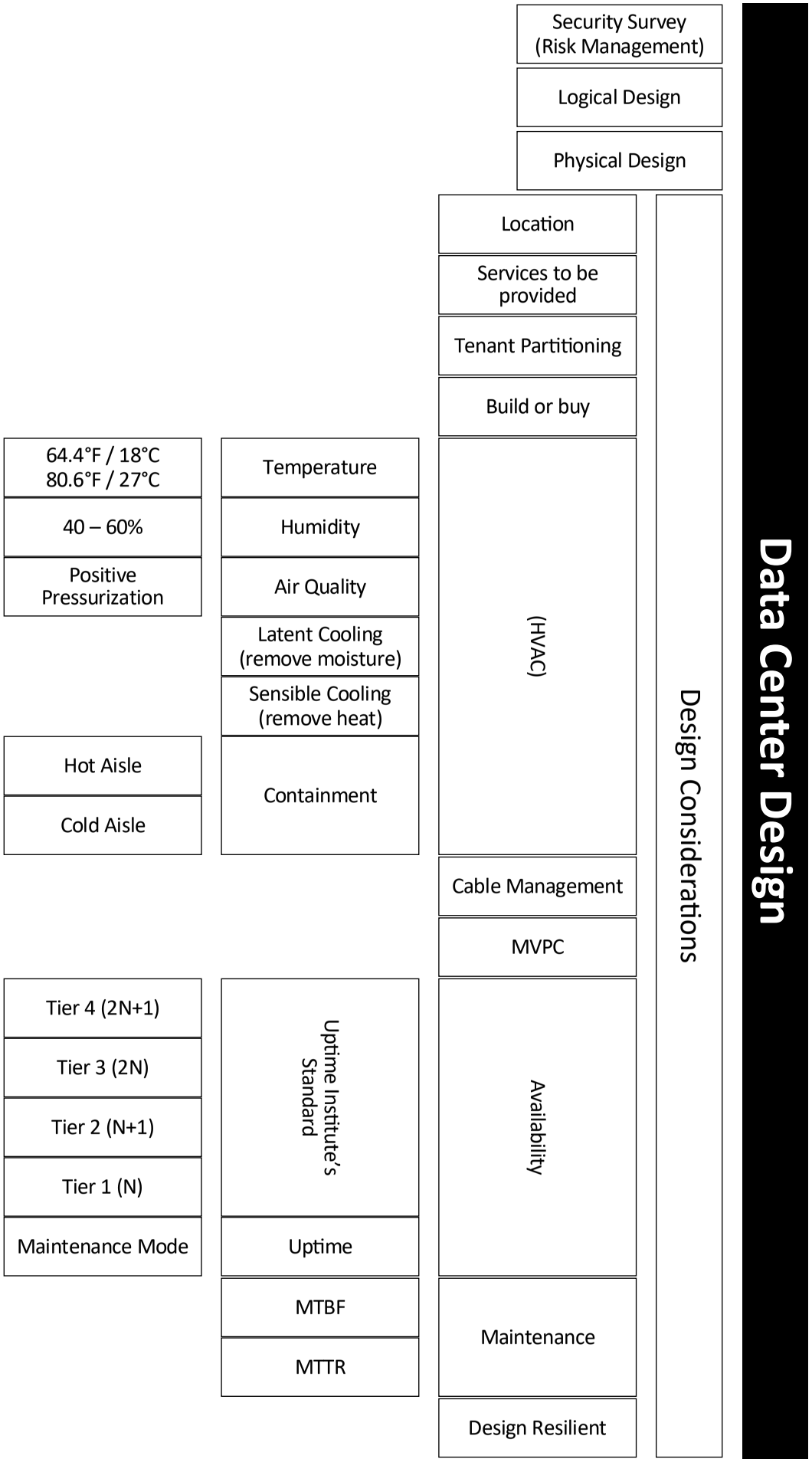
Single most significant difference

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
Design Considerations
Security Survey (Risk Management)
Logical Design
Physical Design
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

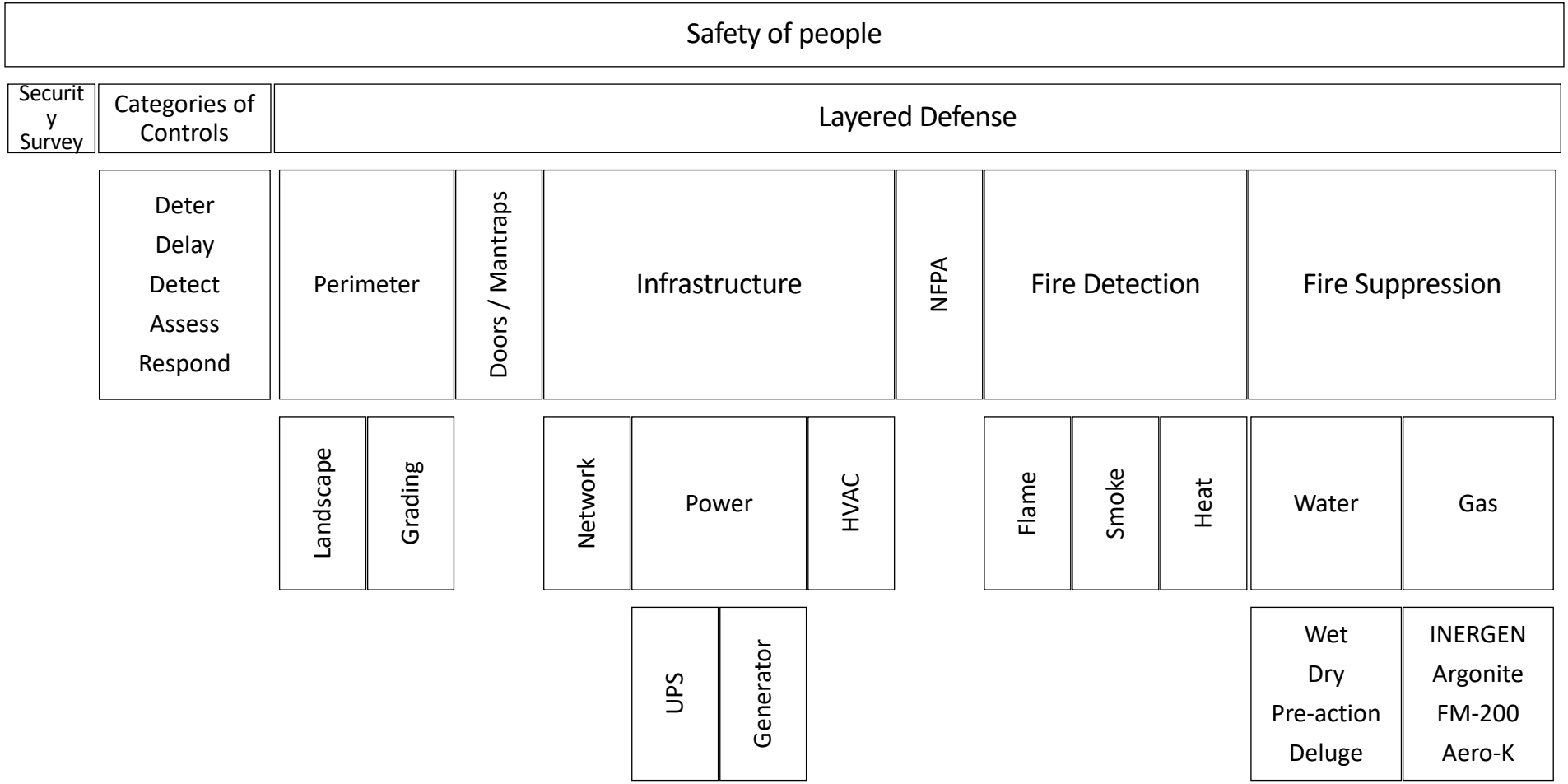
Attack Vectors

Common							Specific to Cloud							
Denial of Service	Malware	System vulnerabilities	XSS, CSRF, SQL Injection, etc.	Malicious insiders	Social engineering	Advanced Persistent Threats	Insufficient Due Diligence	Guest Escape / VM Hopping	Hyperjacking attack	Hyperstack attack	Insecure Interfaces / APIs	Provider's infrastructure	Shared technology	Account hijacking

Risks

Common			Specific to Cloud							
Data Loss / Breach	Data Integrity	Compliance & regulatory	VM Sprawl	Sensitive data within a VM	Dormant VMs	Instant-on gaps	Resource exhaustion	Hypervisor security	Data comingling	Inter-VM communication (blindspots)

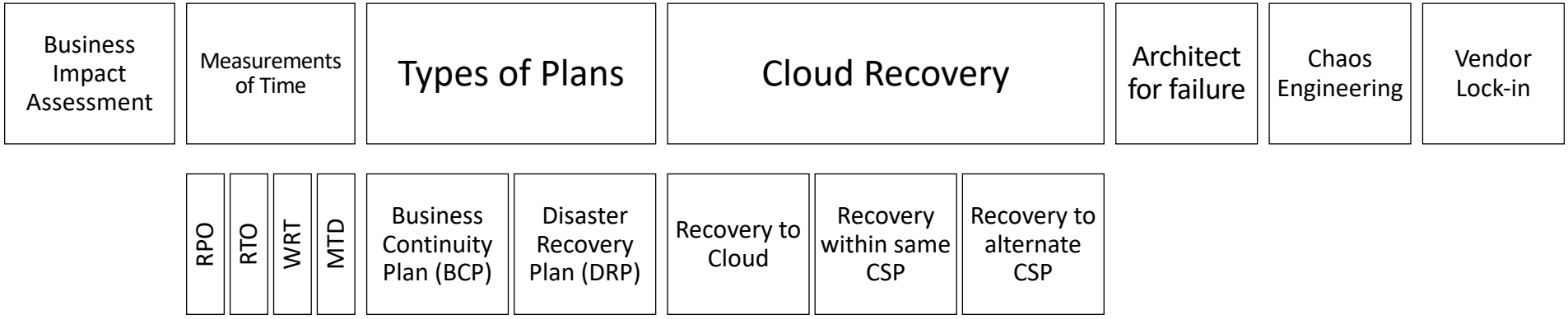
Physical Security



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
      - Stateful matching
    - Anomaly
      - Statistical
      - Protocol
      - Traffic
    - White & Black Lists
    - Sandbox
  - Honeypots & honeynets
  - Ingress vs. Egress
- **Endpoint Security**

Business Continuity Management (BCM)



Domain 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)

"meta-phases" of cloud SDLC

Plan + Mgmt. Approval

Requirements Analysis

Software Development Life Cycle (SDLC)

Operation

Disposal

Secure Design & Development

Secure Deployment

Secure Operations

Design

Development

Testing

Deployment

Waterfall

Agile

DevOps

Cannot go back

Sprints

Scrum Master

Combine Dev, QA & Ops

DevOps Security

CI / CD

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	Authenticity	Non-Repudiation		Access Control
	= Hashing		Origin	Delivery	

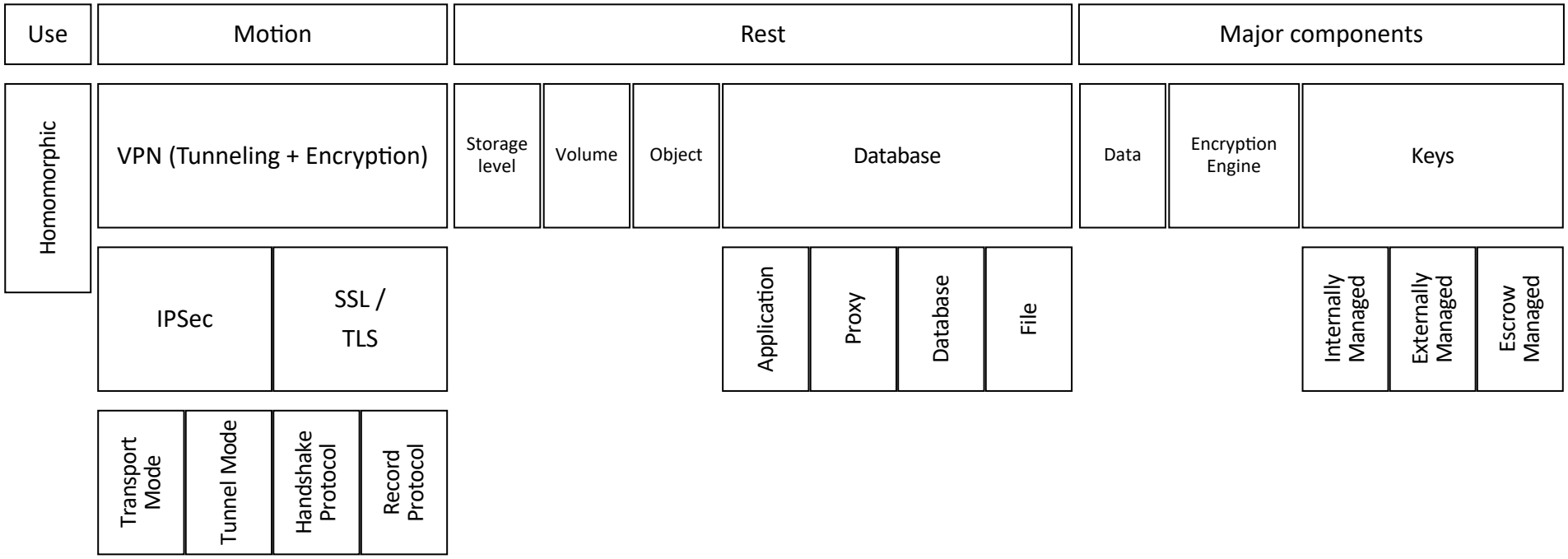
Cryptography

One-way	Two-way		Digital Signatures	Digital Certificates
Hashing	Symmetric	Asymmetric	Integrity Authenticity Non-repudiation	Verify owner of public key
				X.509

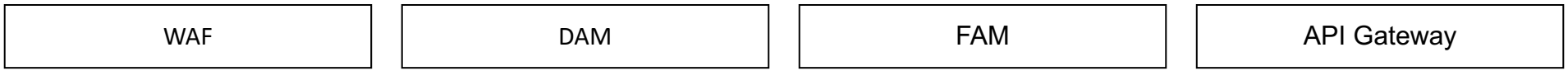
Key Management

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

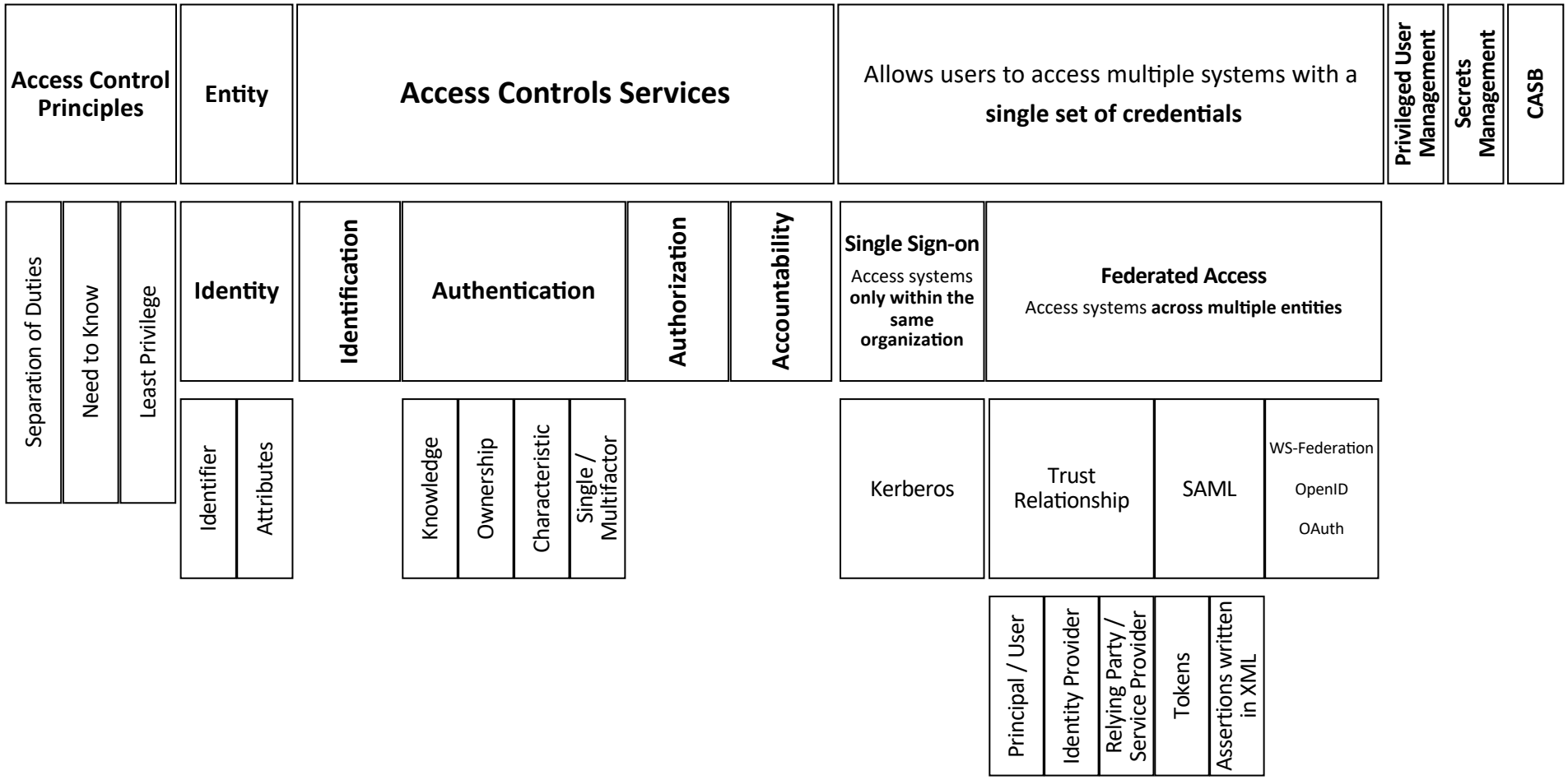
Crypto in the Clouds



Proxies

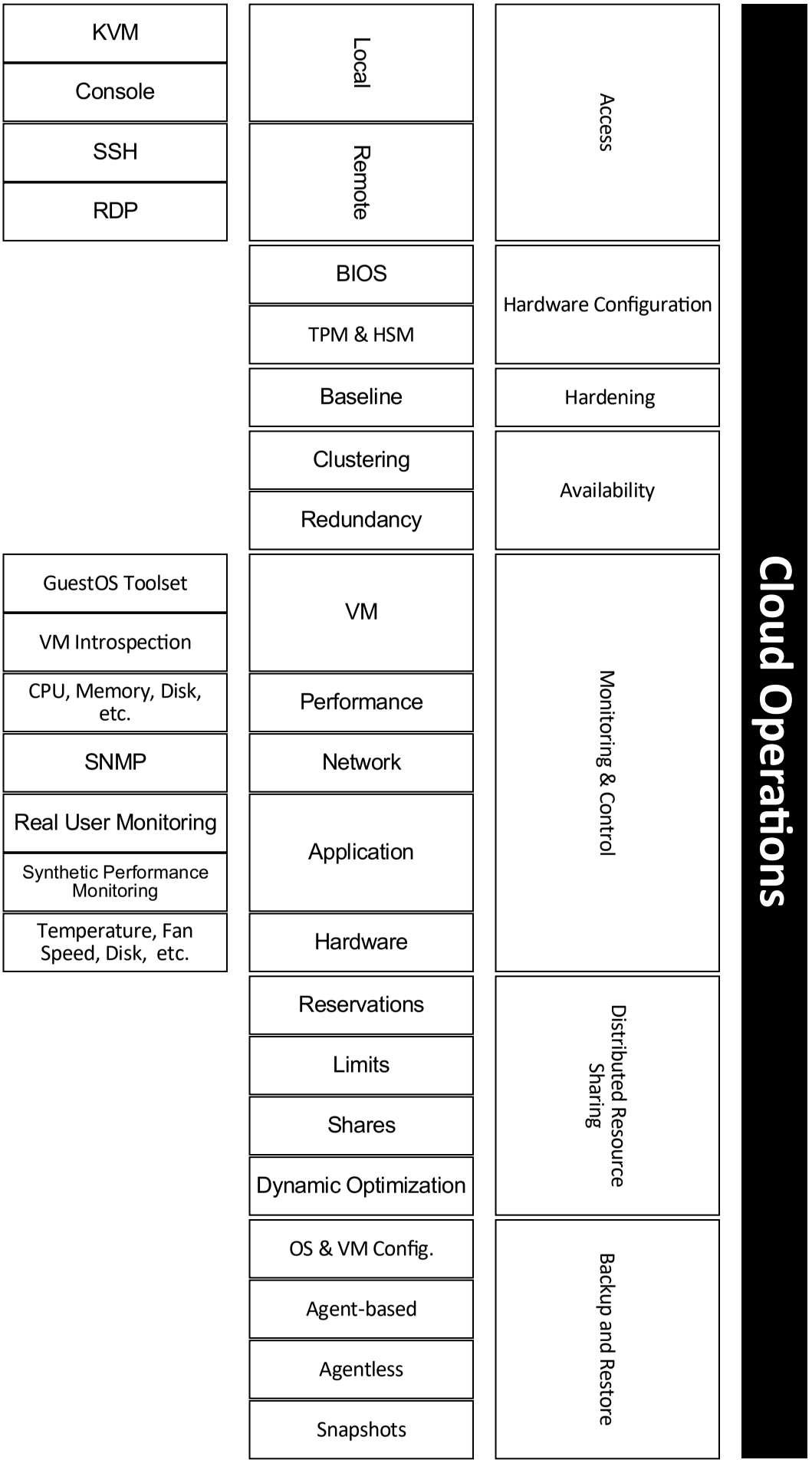


Access Control



Domain 5

Cloud Security Operations


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

IT Service Management

- Strategy
- Design
  - Availability
  - Capacity
  - Continuity
  - Service Level
    - Contract
      - Negotiable
      - Non-negotiable
      - Click-wrap Agreements
    - SLA, PLA, & OLA
- 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 Service Improvement
- Continual Improvement

Investigations

Secure the Scene	Collect & Control Evidence									Rules of Evidence					Document & Report
	Sources of Evidence					Forensics Support			Chain of Custody	Authentic	Accurate	Complete	Convincing	Admissible	
	Oral / Written statements	Documents	Digital Forensics		eDiscovery	SaaS	PaaS	IaaS							
			Snapshotting MVs	Live Evidence (Volatile)	Metadata on Infrastructure Configuration	ISO 27050	Rely entirely on CSP	CSP for Infrastructure & Consumer for their apps	CSP for Infrastructure & Consumer for their virtual systems and apps						

Domain 6

Legal, Risk and Compliance

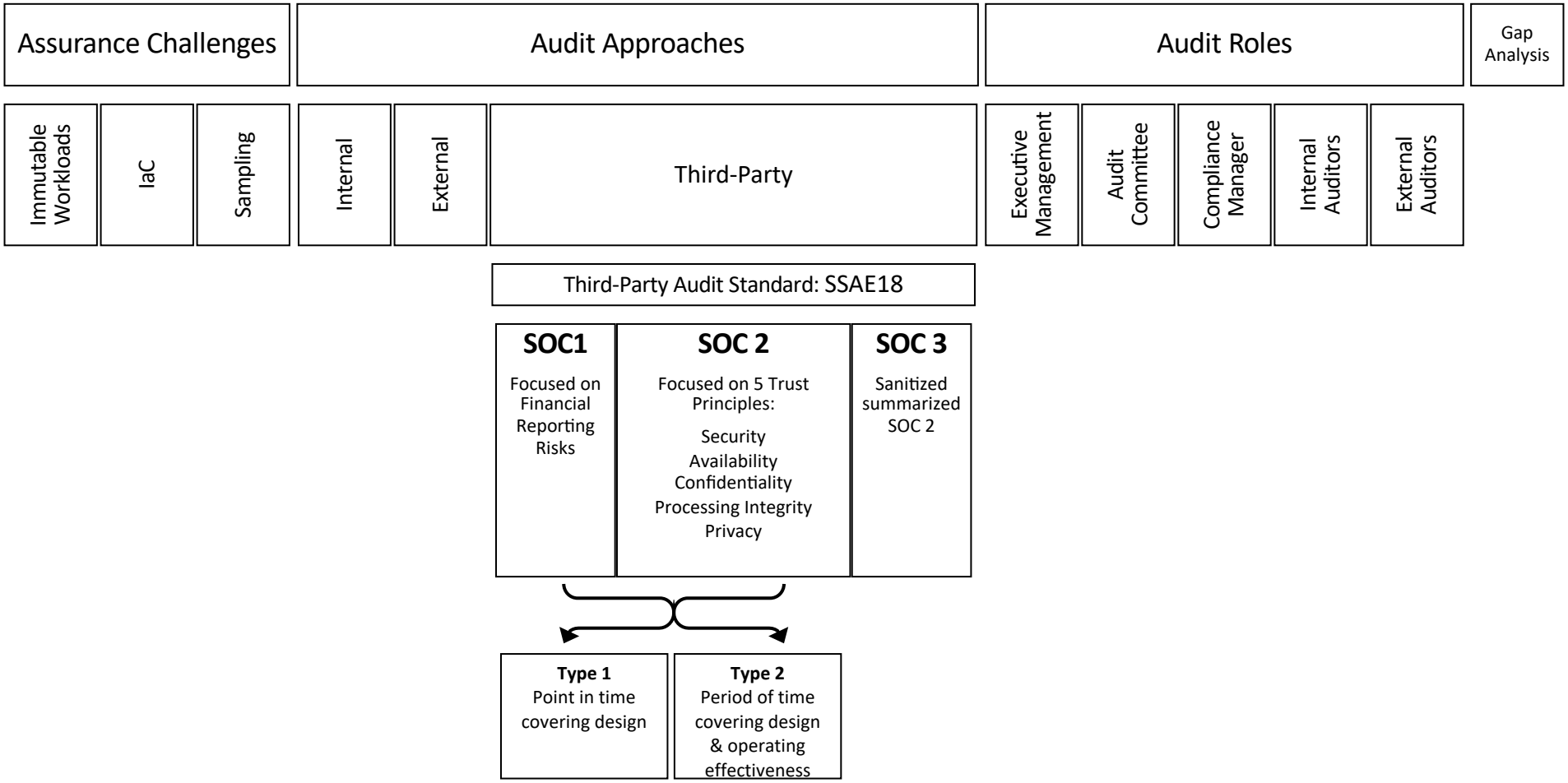
Privacy

- 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

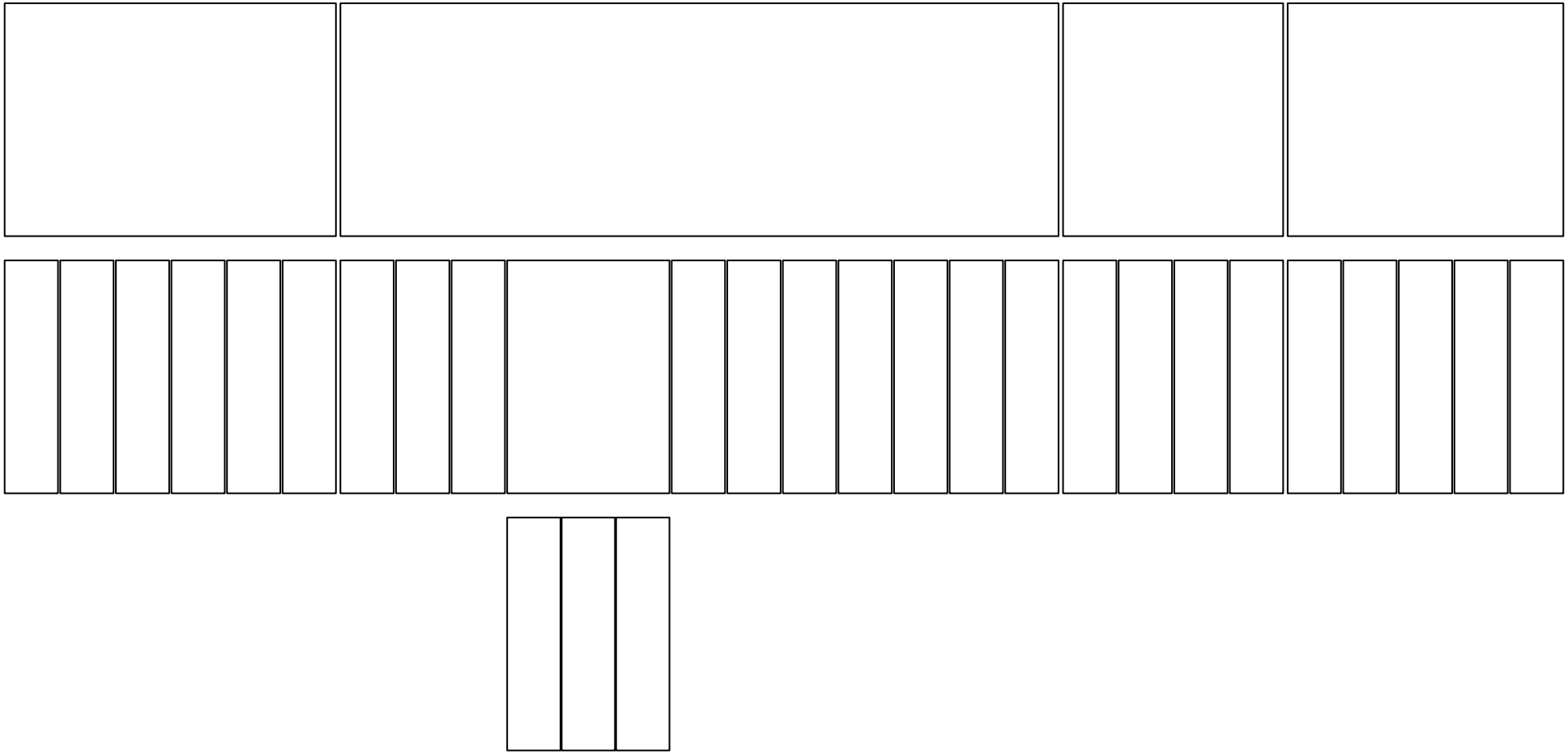

Assurance Challenges
Audit Approaches
Audit Roles
Gap Analysis
Immutable Workloads
IaC
Sampling
Internal
External
Third-Party
Executive Management
Audit Committee
Compliance Manager
Internal Auditors
External Auditors
Third-Party Audit Standard: SSAE18
SOC1
Focused on Financial Reporting Risks
SOC 2
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

Printable Blank CCSP MindMaps

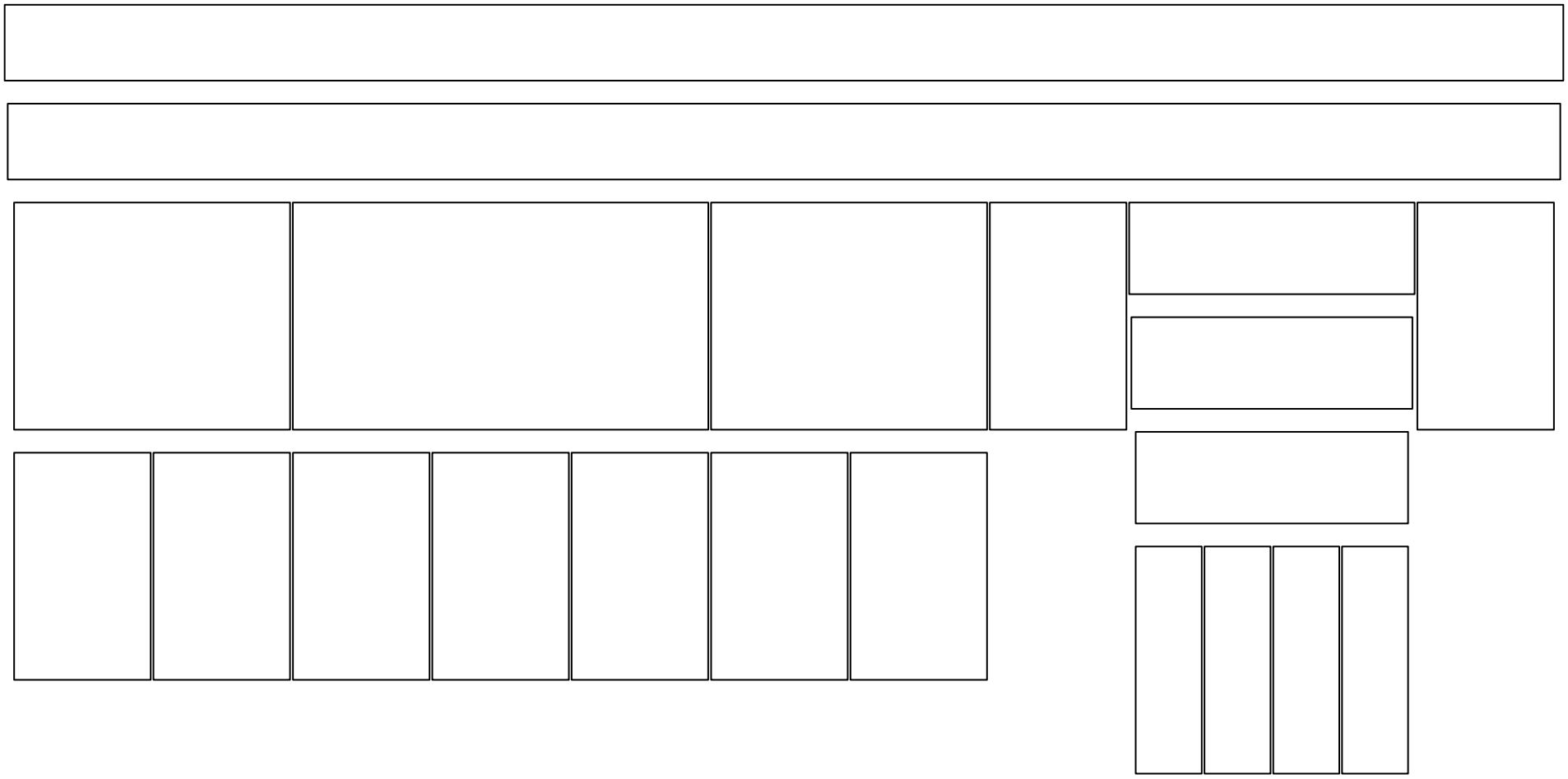
Print out the following blank MindMaps and fill them in as your watch our MindMap videos!

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

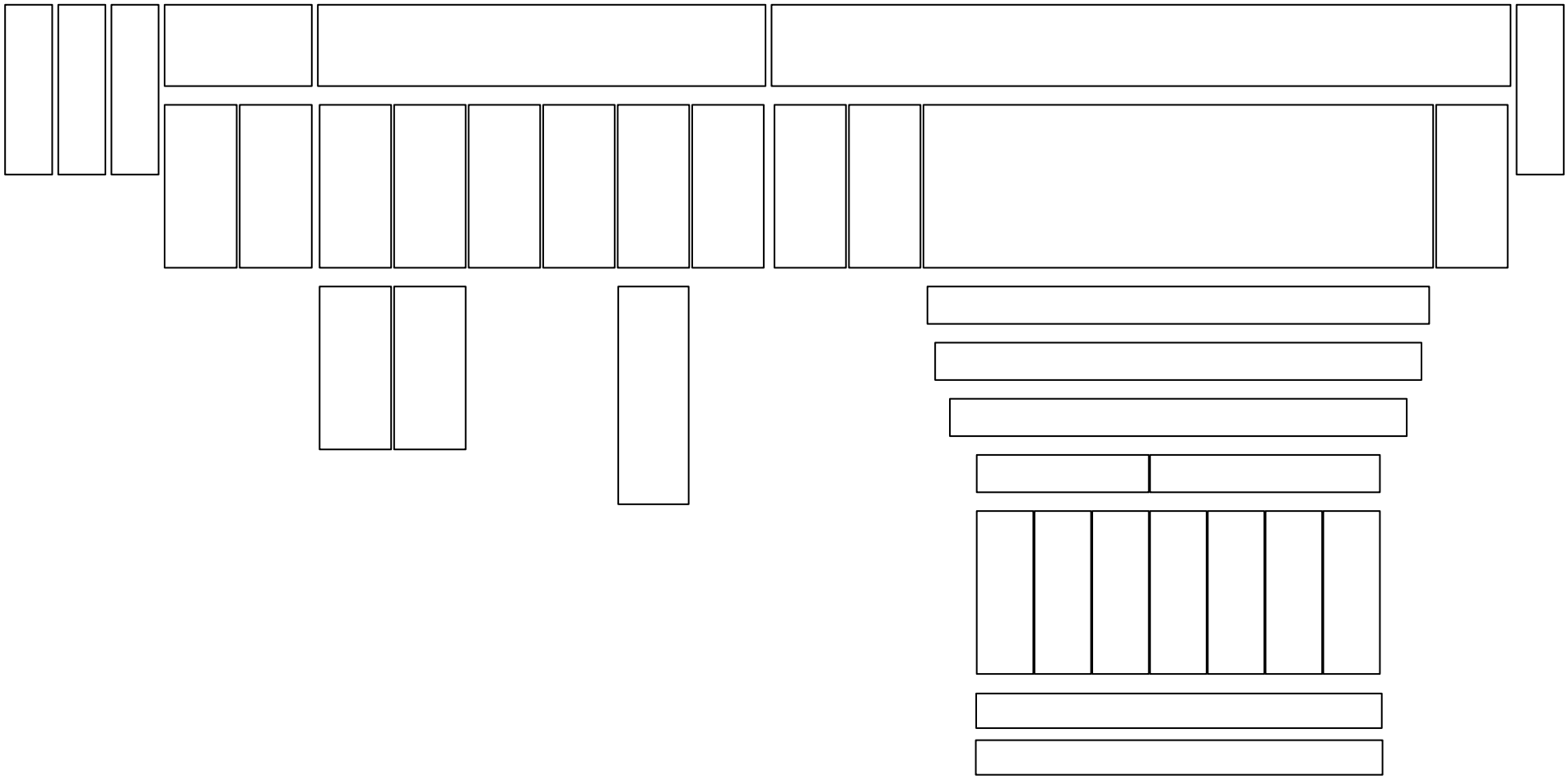
Cloud Computing



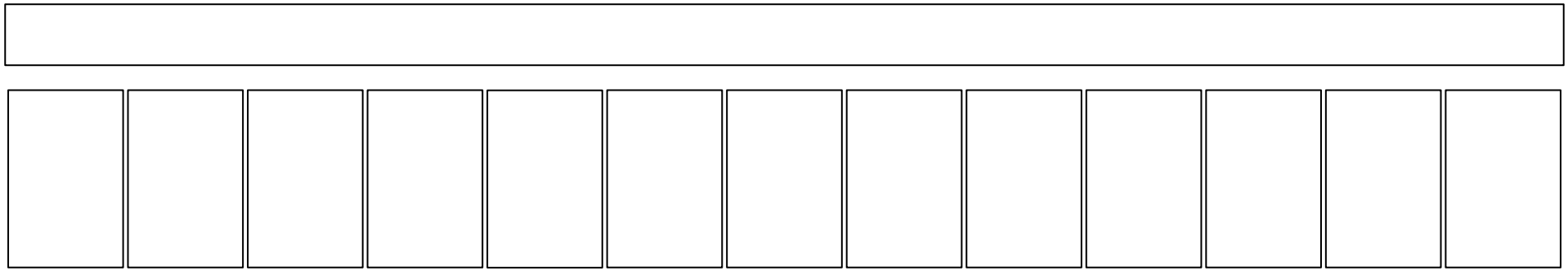
Alignment of Security Function to Business Strategy



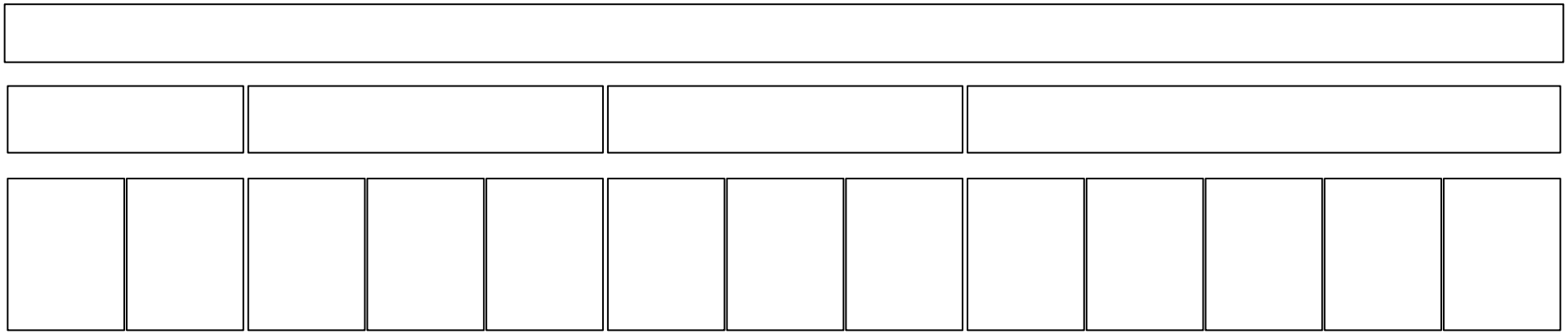
Risk Management



Cloud Shared Considerations



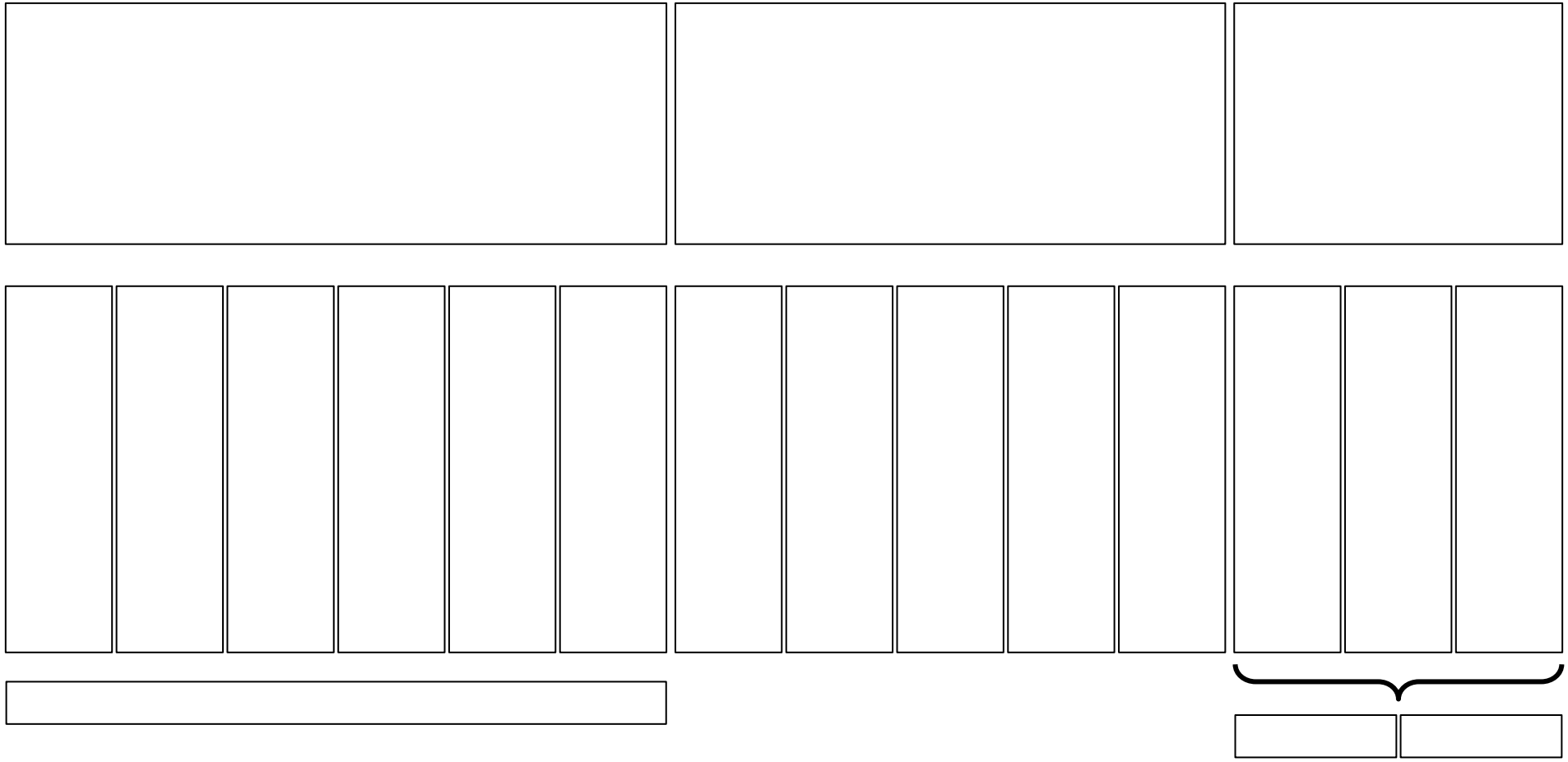
Frameworks



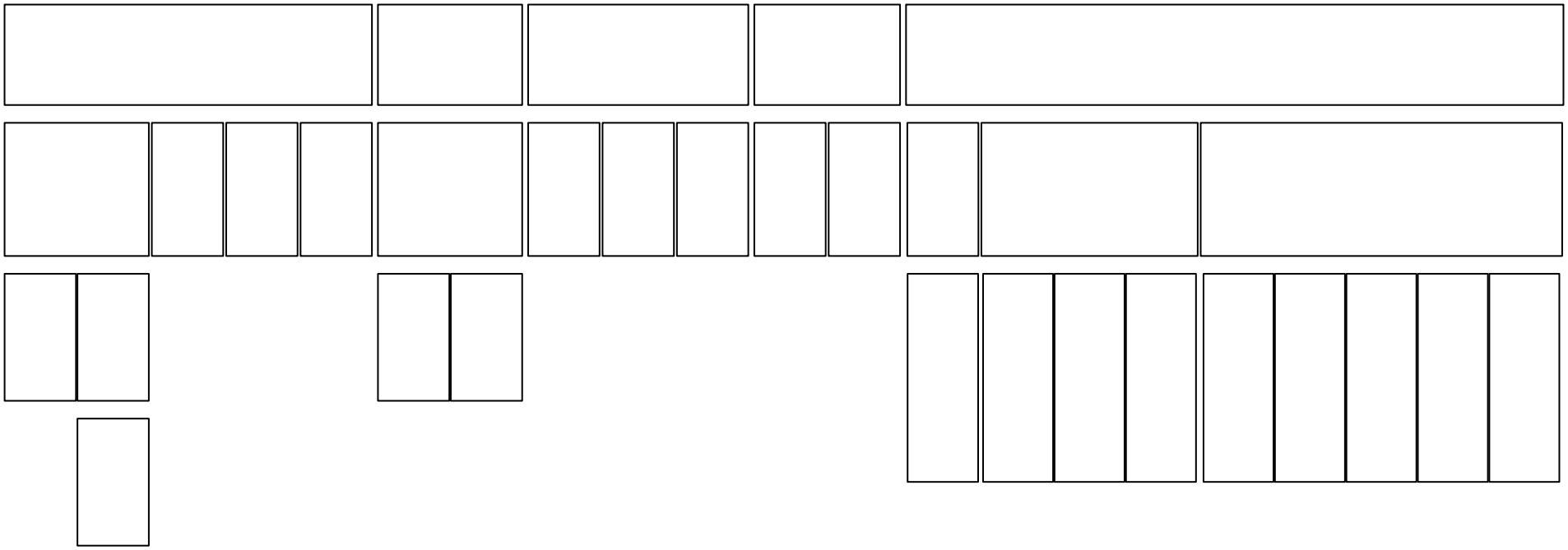
Cost Benefit Analysis

Evaluation Criteria

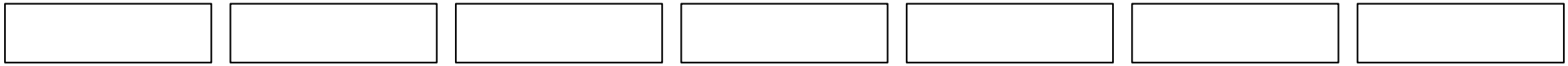
Cloud Data Lifecycle



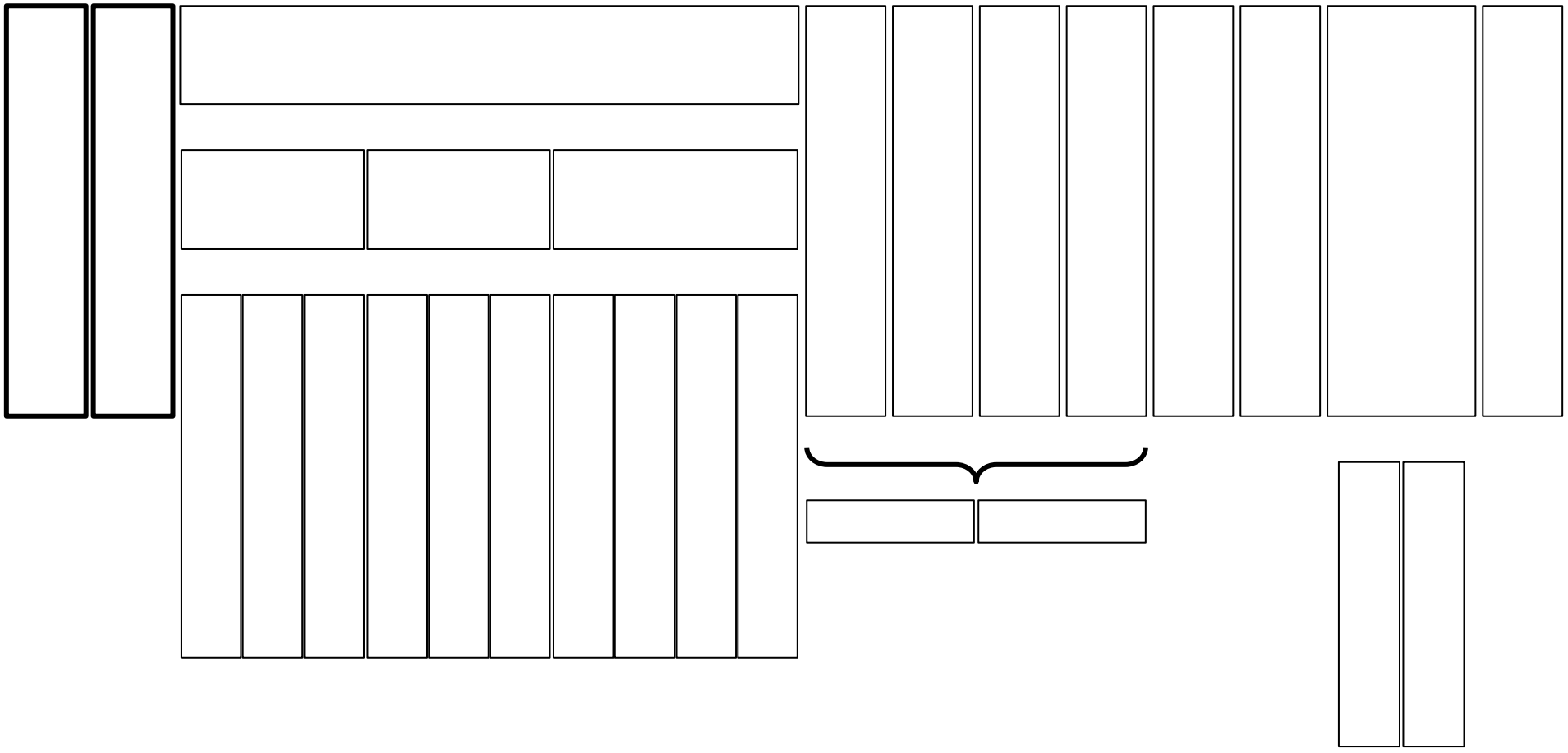
Cloud Data Storage



Threats to Storage



Data Security Strategies

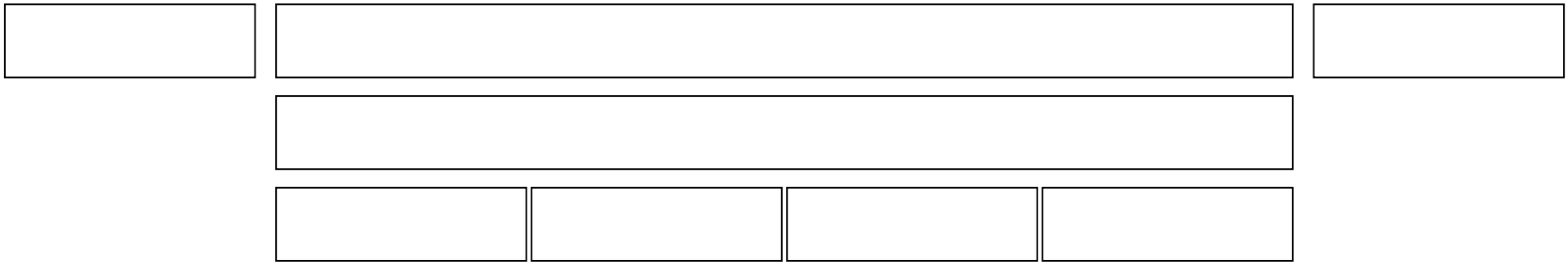


Data Discovery

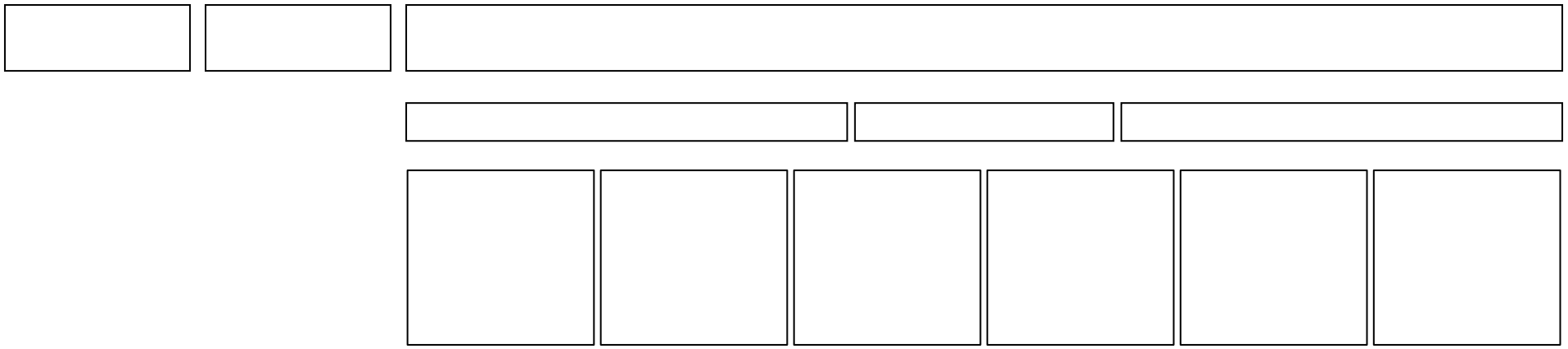
Asset Classification

Log Review & Analysis

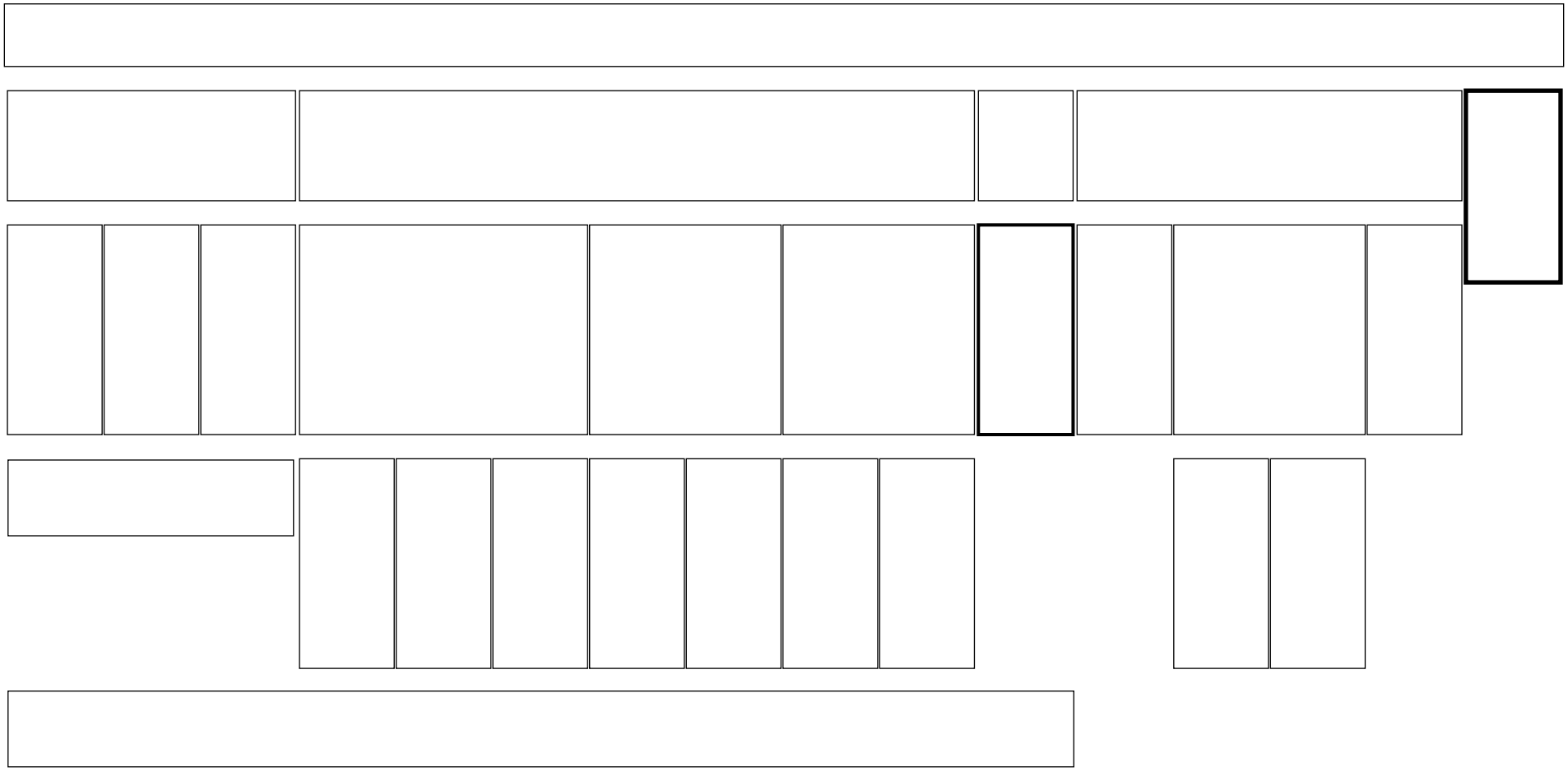
Digital Rights Management (DRM)



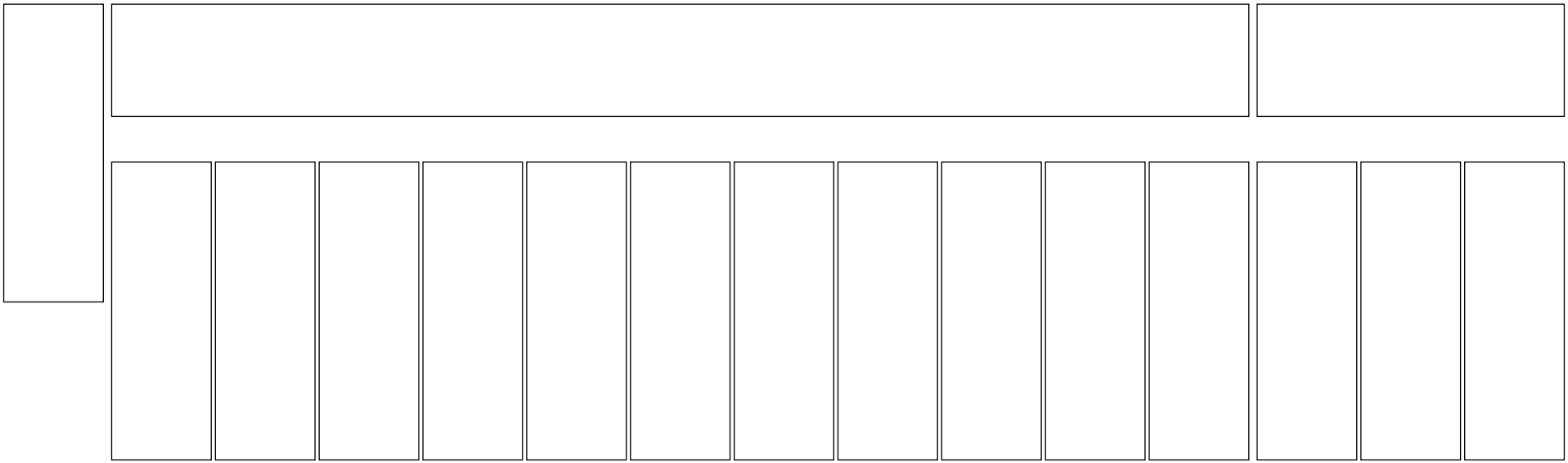
Data Retention, Archiving & Deletion



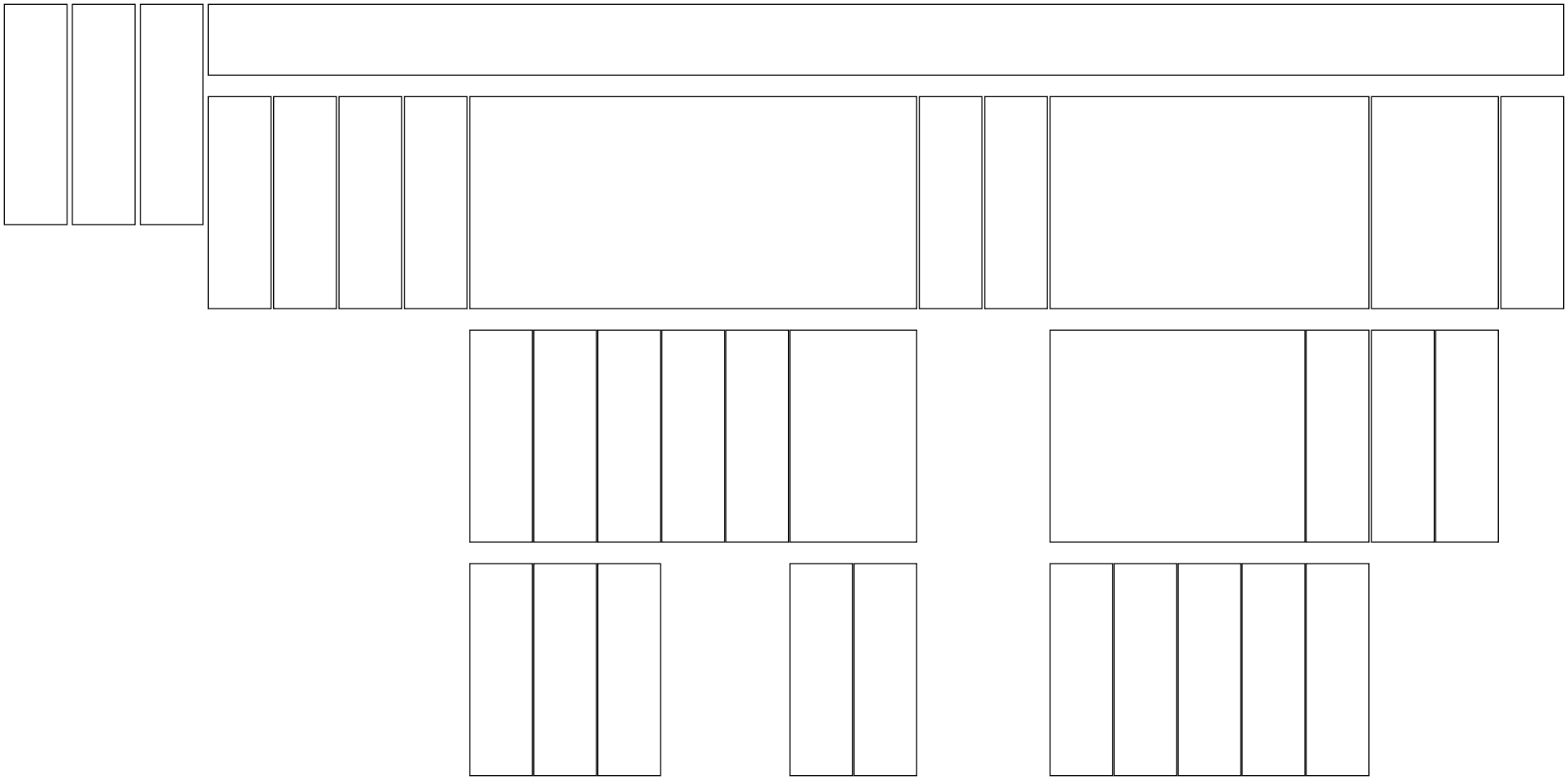
Cloud Infrastructure Components



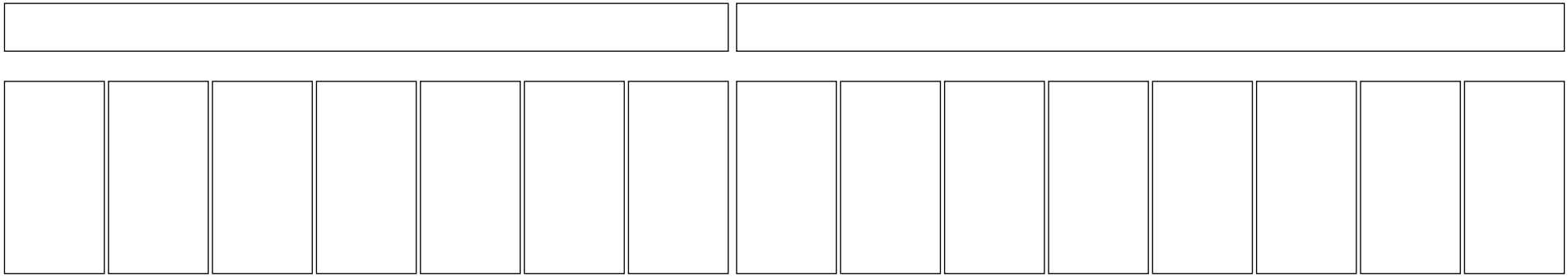
Management Plane



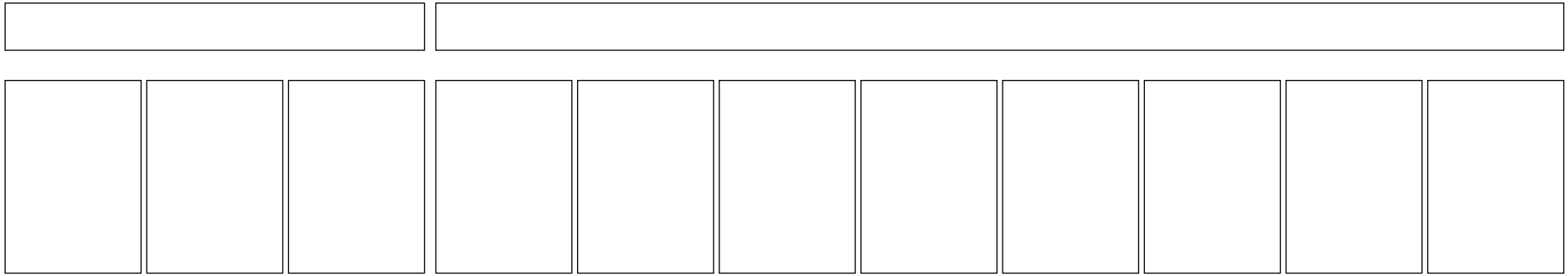
Data Center Design



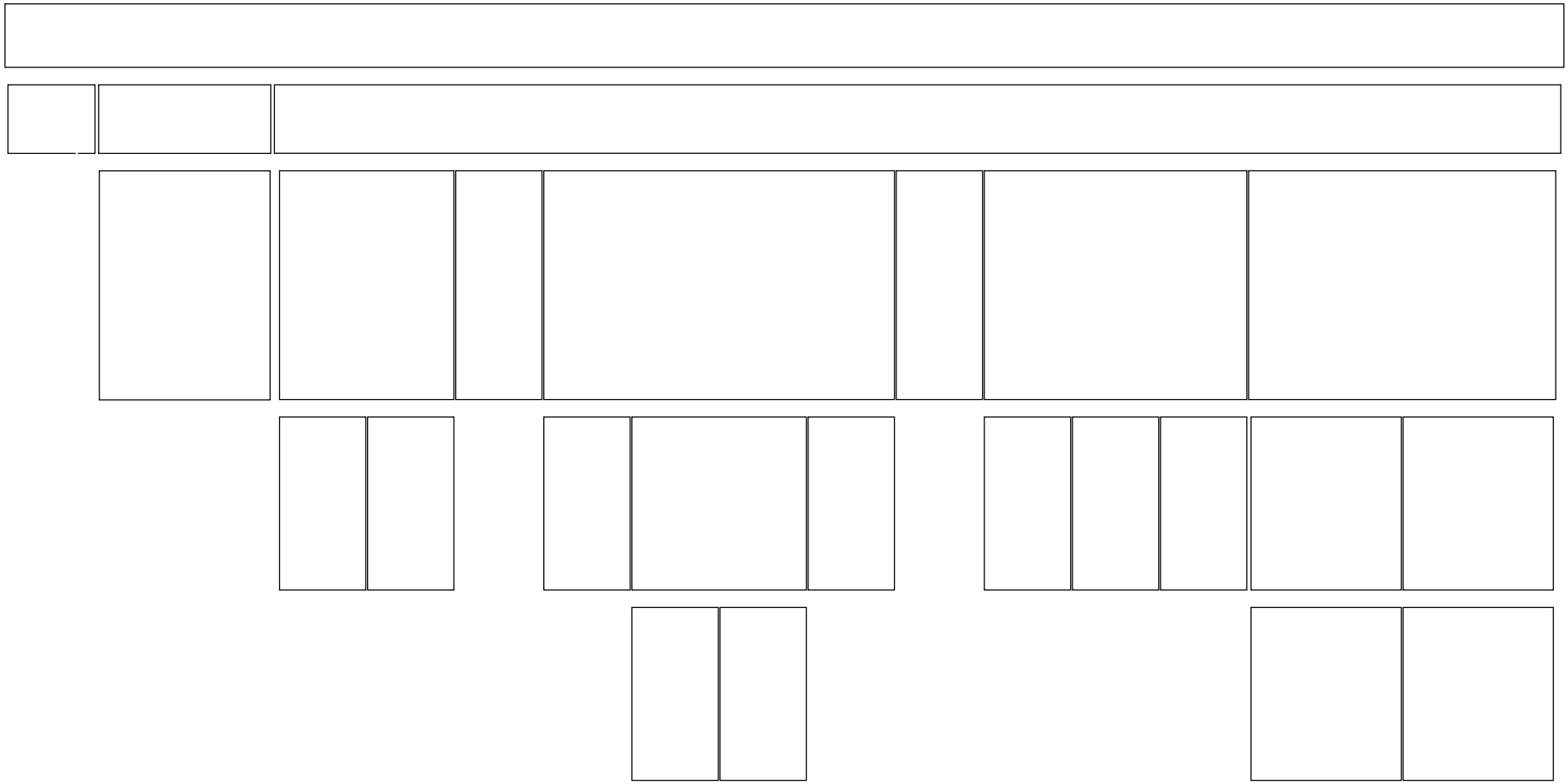
Attack Vectors



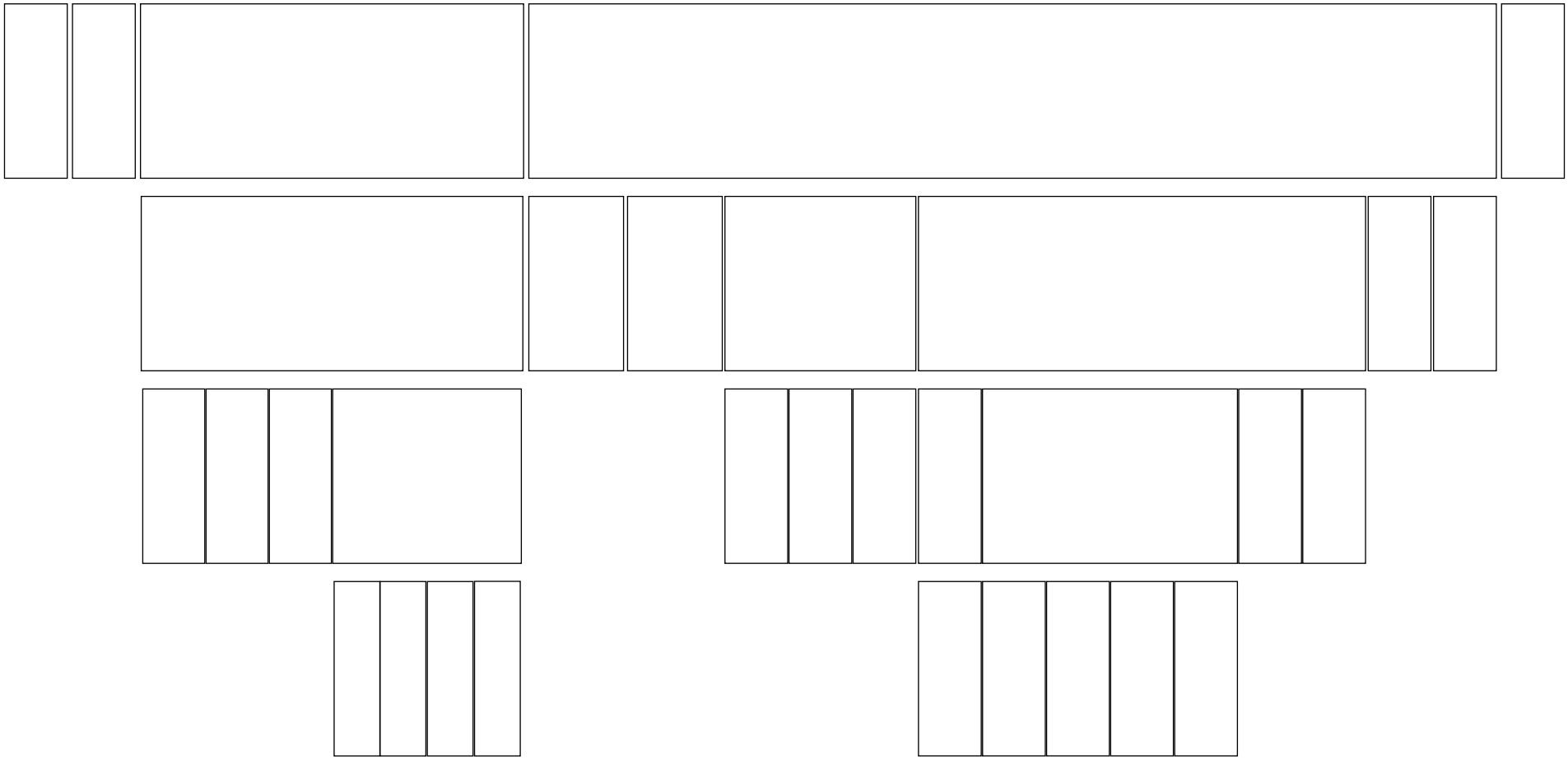
Risks



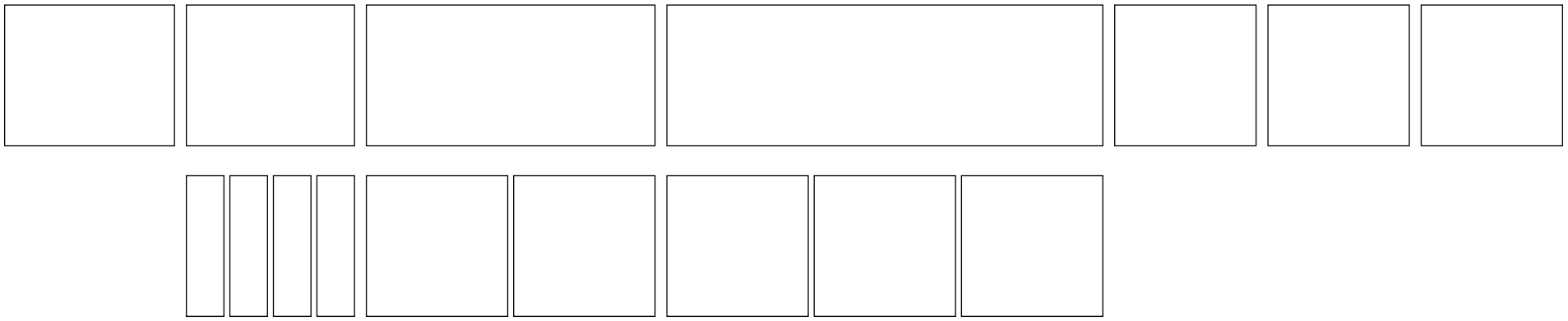
Physical Security



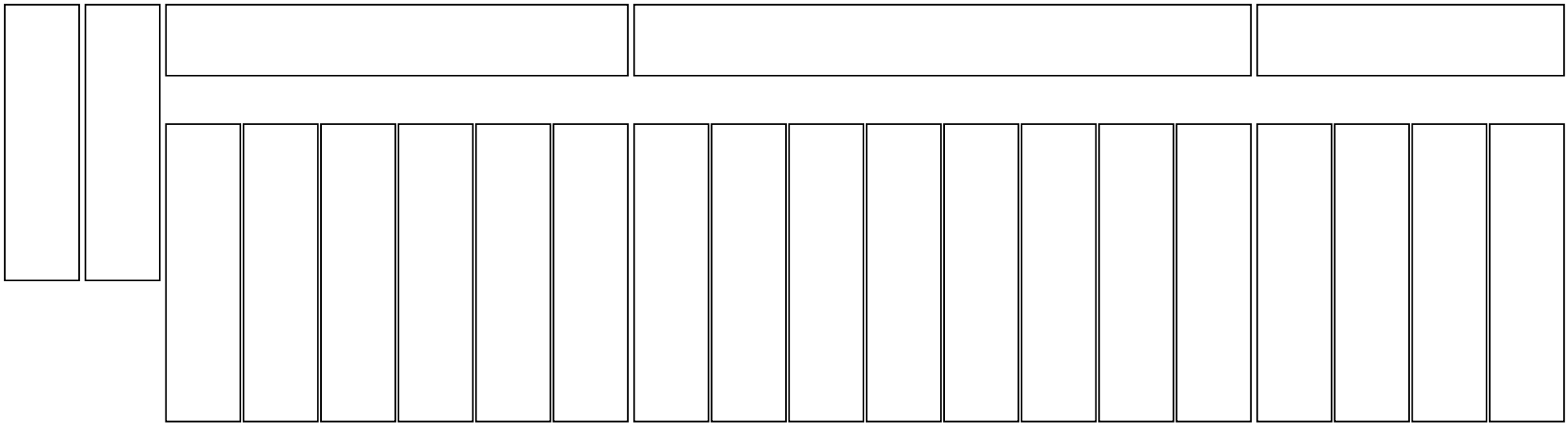
Network Defense



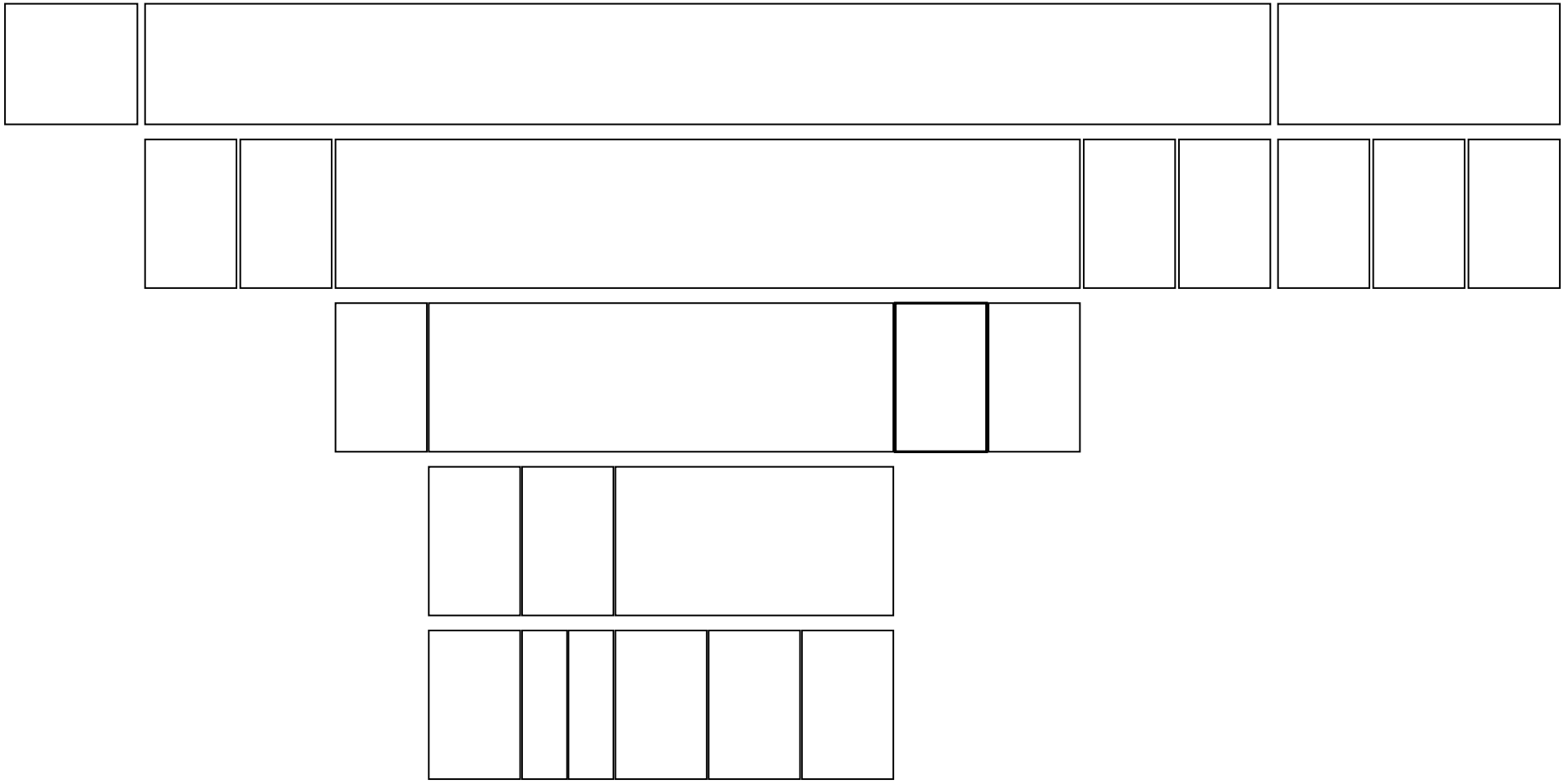
Business Continuity Management (BCM)



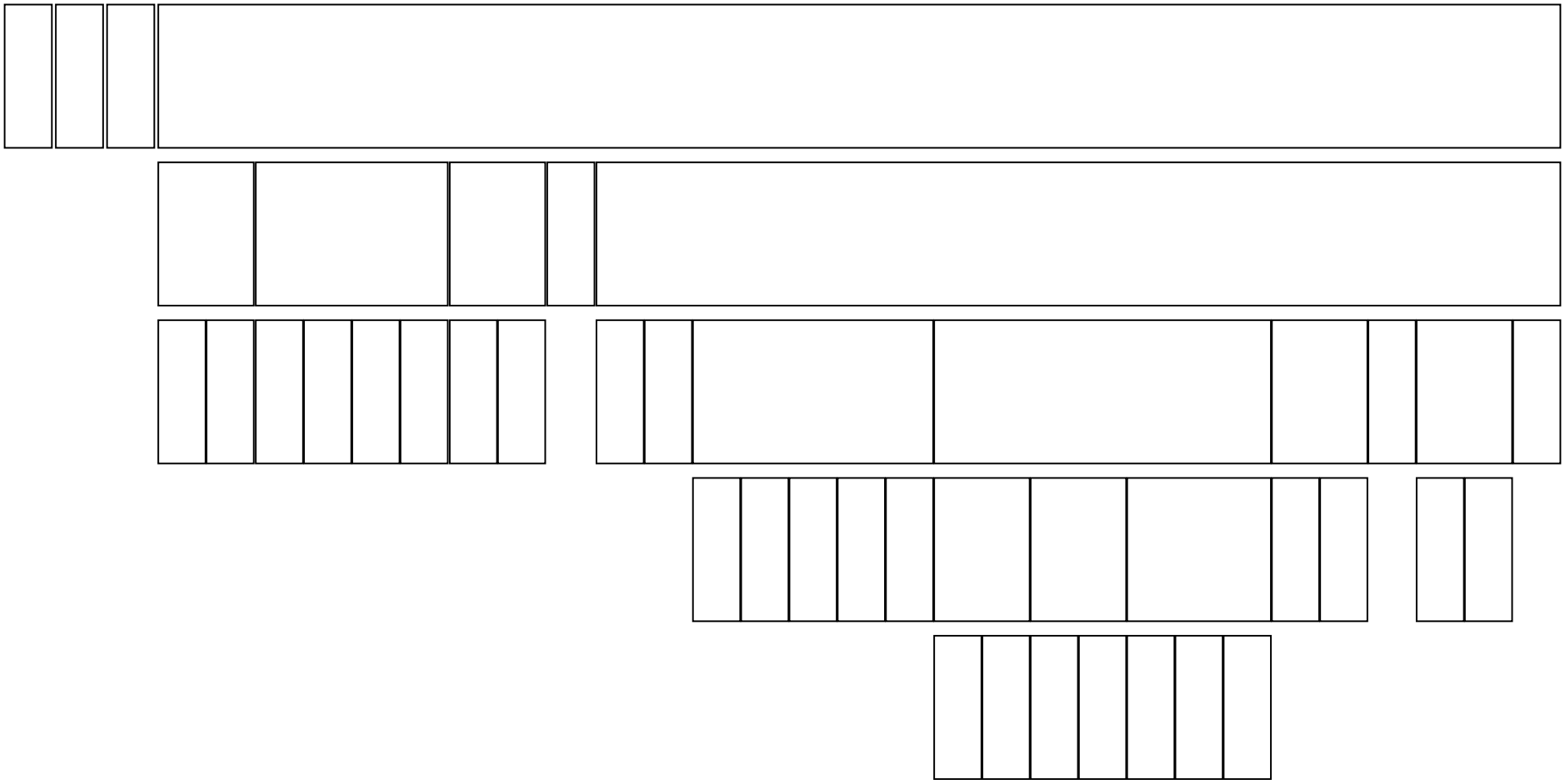
Cloud Development



Secure Software Development

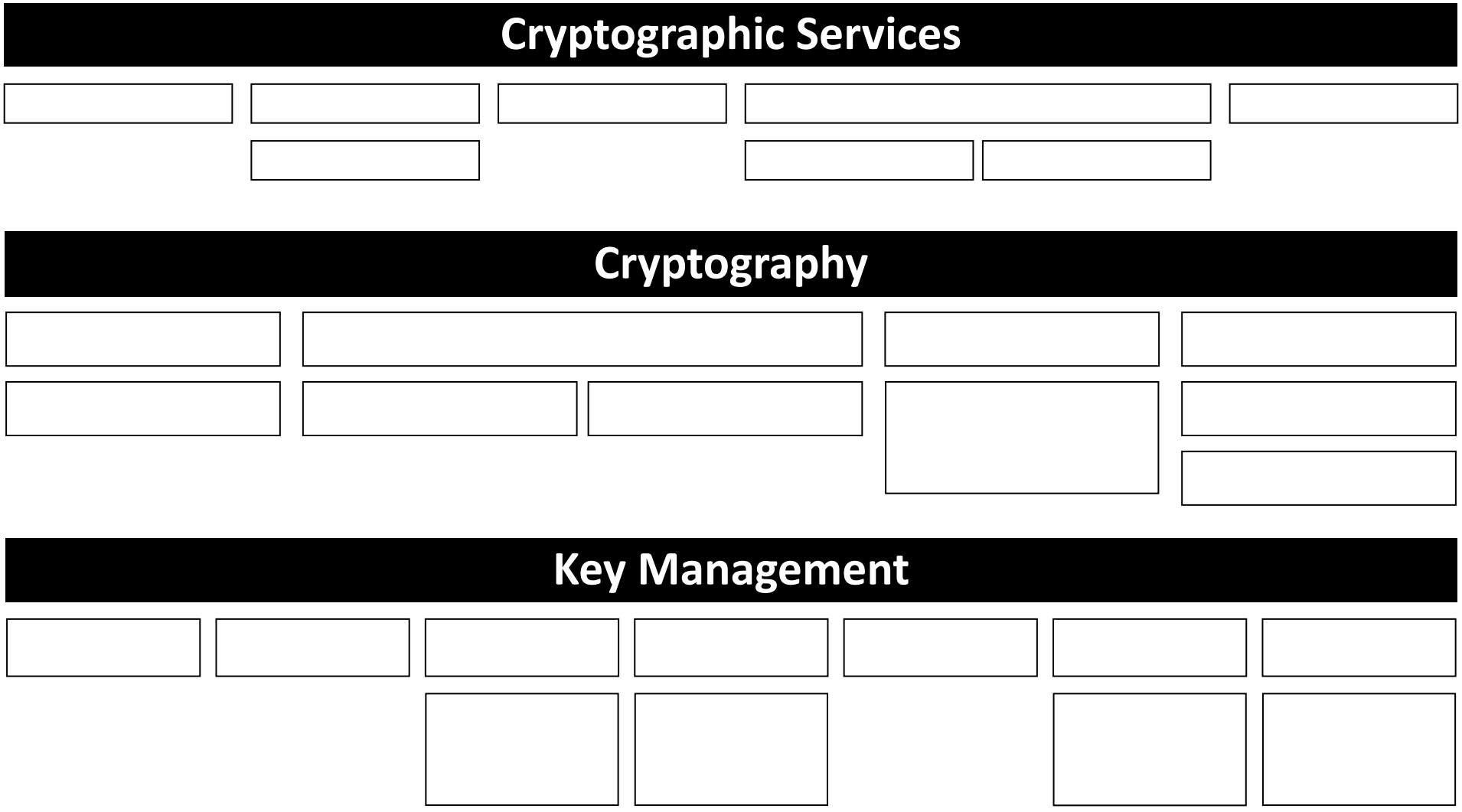


Security Assessment and Testing

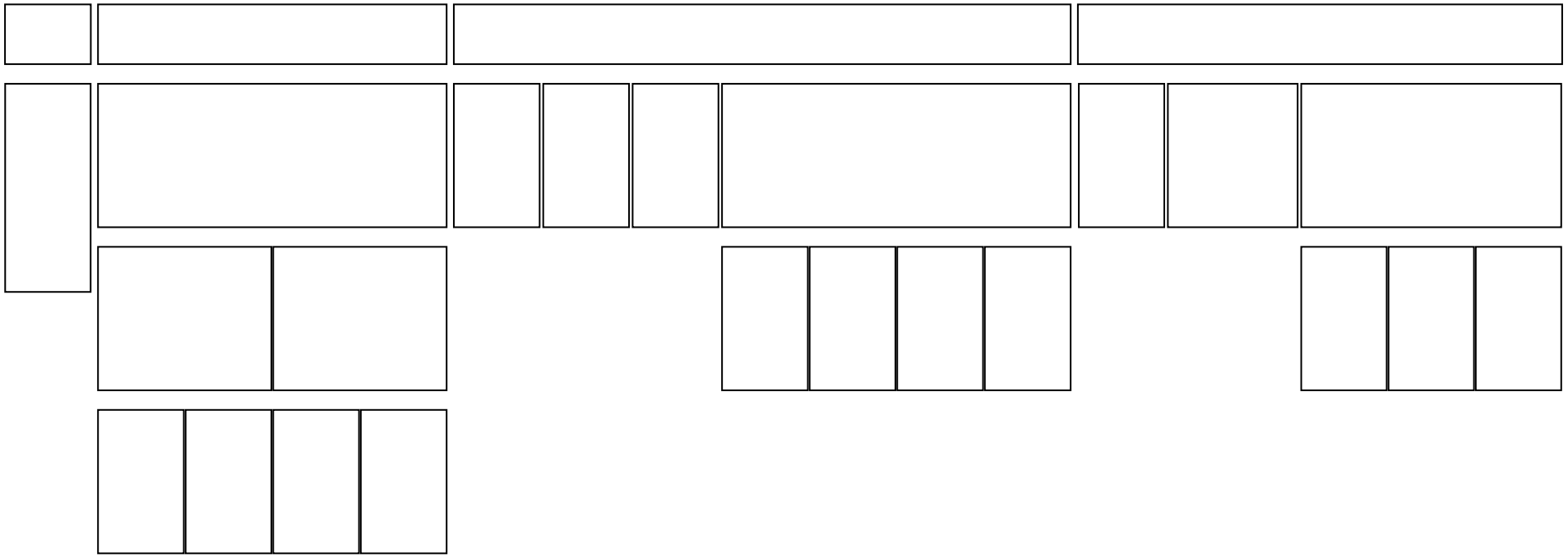


Common Vulnerabilities & Threat Modeling

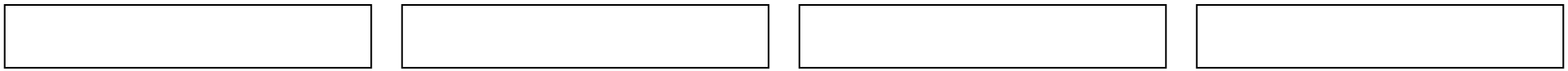
Verified Secure Software


Cryptographic Services
Cryptography
Key Management

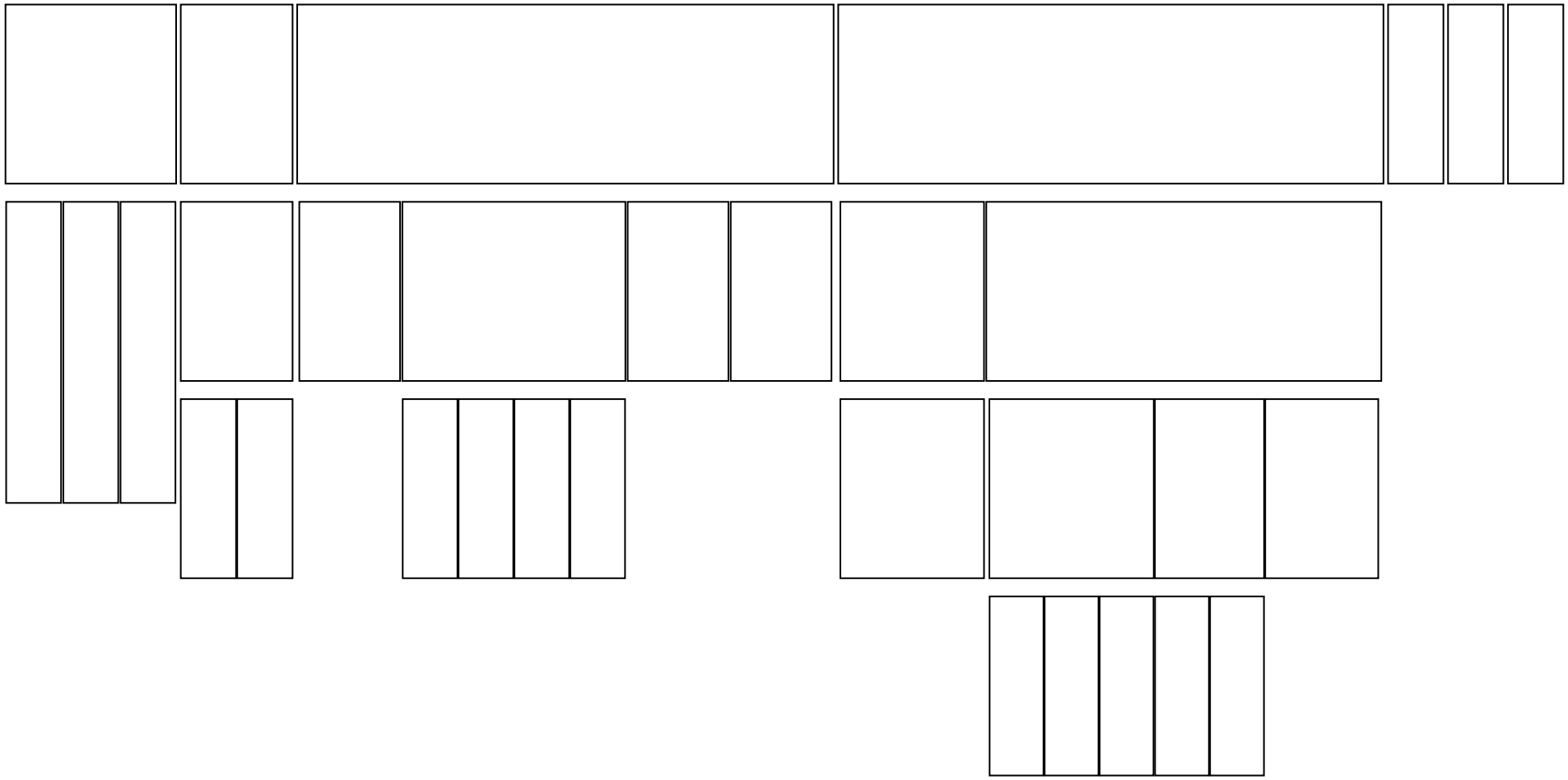
Crypto in the Clouds



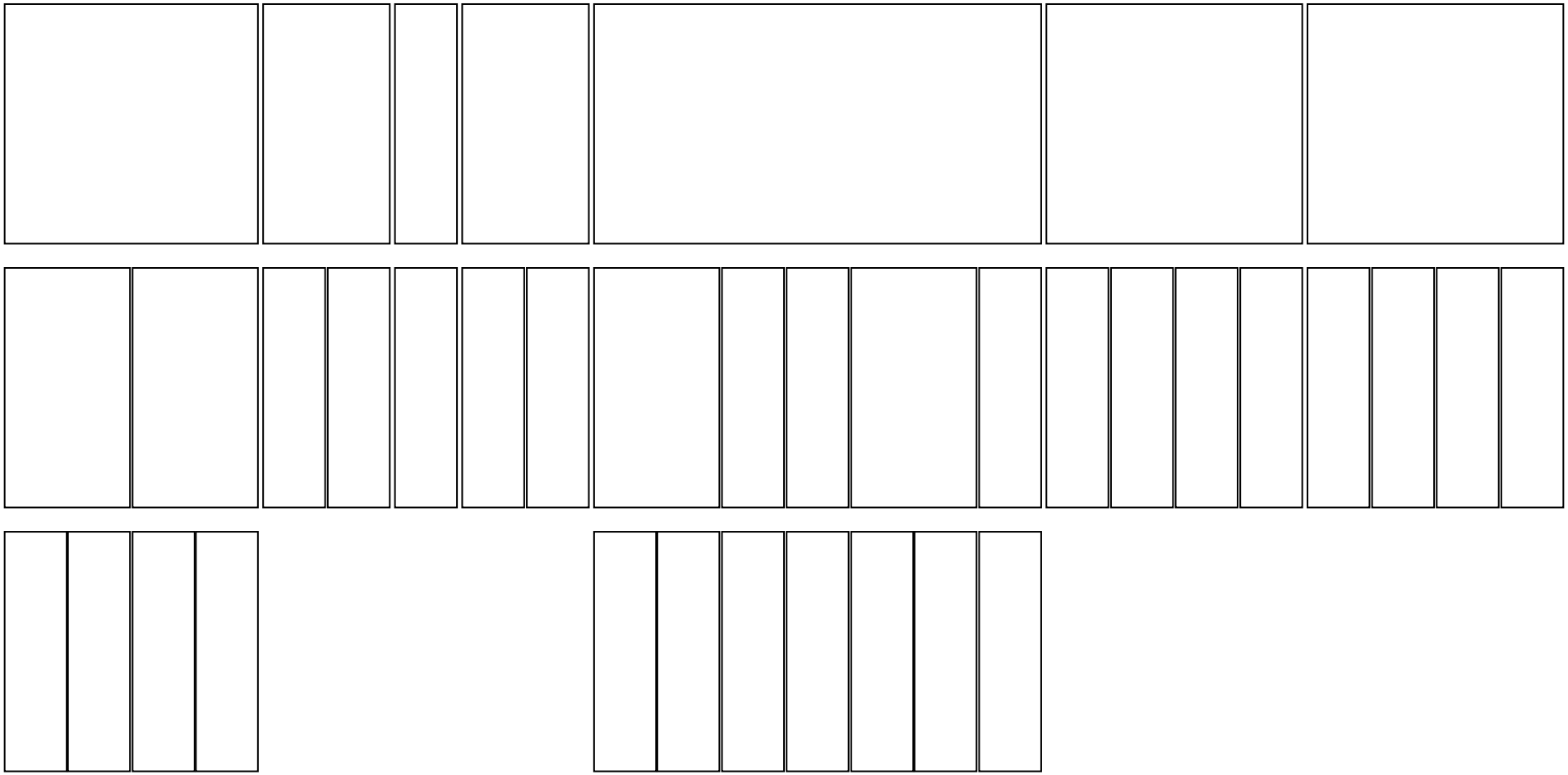
Proxies



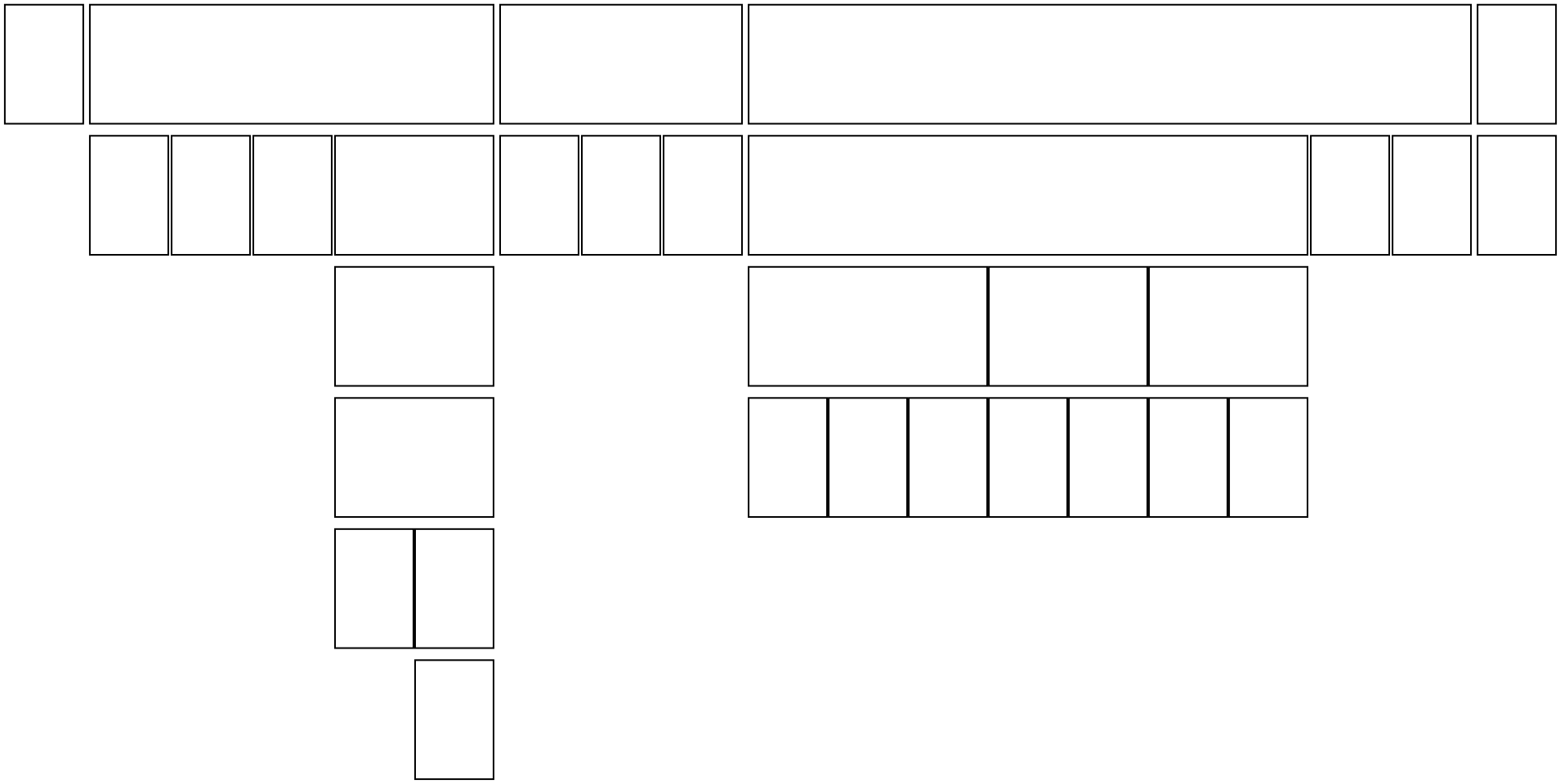
Access Control



Cloud Operations

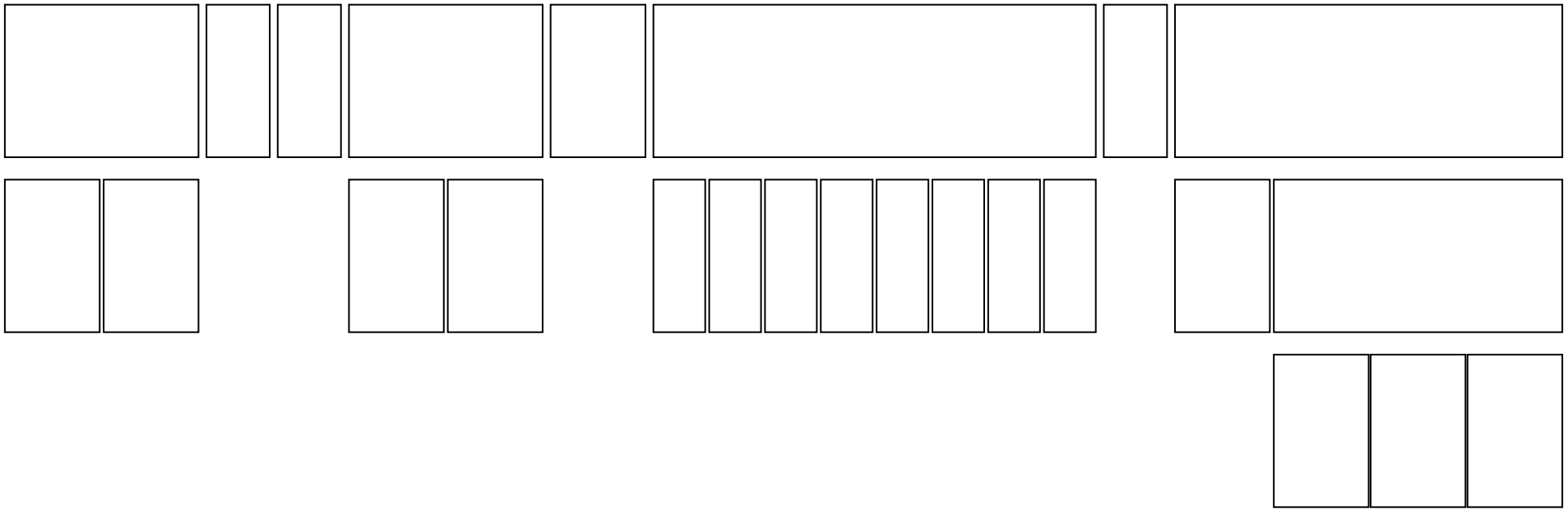


IT Service Management



Investigations

Privacy



Outsourcing & Cloud Contracts

Cloud Audit