



DESTINATION
CERTIFICATION

CCSP

MindMaps

Domain 1

Cloud Concepts, Architecture and Design



Cloud Computing

Characteristics						Roles										Service Models				Deployment Models					
On-Demand Self Service	Broad Network Access	Resource Pooling	Rapid Elasticity	Measured Service	Multi-tenancy	Accountability vs. Responsibility	Customer / Consumer	Provider	Broker	Cloud Developer	Cloud Administrator	Cloud Service Manager	Cloud Service Business Manager	Cloud Service Deployment Manager	Cloud Service Integrator	Cloud Regulator	IaaS	PaaS	SaaS	XaaS: IDaaS, NaaS, CompaaS	Public	Private	Community	Hybrid	Multi
						Aggregation																			
						Arbitrage																			
						Intermediation																			

Alignment of Security Function to Business Strategy

Corporate Governance

Security Governance

Focus of Security

Goals of Information Security

Clearly Defined Roles
& Responsibilities

Privacy

Corporate Laws

Overarching Security
Policy

Risk Management

Functional Security
Policies

Enable Business

Increase Value

Confidentiality

Integrity

Availability

Accountability

Responsibility

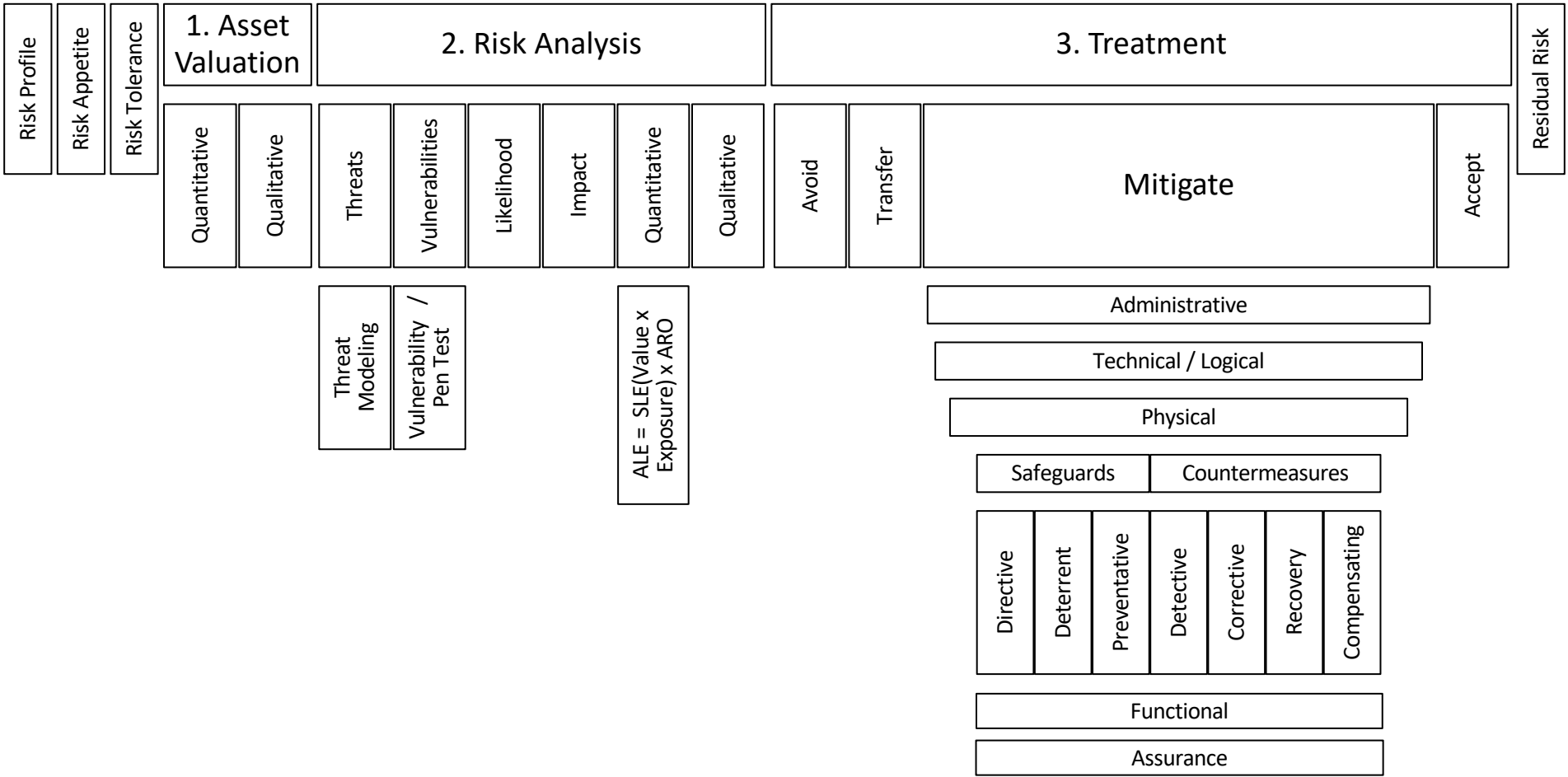
Standards

Procedures

Baselines

Guidelines

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
(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

Accreditation

Common Criteria

FIPS 140-2

EAL1 – EAL7

Levels 1 - 4

AI/ML Foundations, Risks, and Governance

AI systems need validated data, ongoing monitoring, and ethical/legal guardrails.

AI and ML Fundamentals		Cloud Threat Detection		Data Sources		Ethical Concerns in AI				Regulatory Requirements																													
Artificial Intelligence		AI Use Cases		Detection		Response and Resilience		Data Origin and Integrity		Data Preparation and Quality		Model Assurance		Privacy Preservation		Misuse		Dual-use Risk		Bias		Decision-making		Regulatory Landscape															
Machine Learning		Inputs and Monitoring		Techniques and Metrics		Automated Response		Data Provenance		Training Data Integrity		Threats		Feature Engineering		Model Validation		Automation Bias		Confirmation Bias		Historical Bias		Sampling Bias		Automated Decision-making		Human Oversight		EU AI Act		Other Regulation		AI-adjacent Regulation		Frameworks		Governance and Documentation	
Deep Learning		Threat Intelligence Feeds		Real-Time Monitoring		Behavioral Baselines		Anomaly Detection		Data Poisoning		HITL		HOTL		HOOTL		Brazil		Colorado		Texas		China		GDPR and AI Alignment		Sector-Specific Obligations		NIST AI RMF		DPIA		FRIA		Algorithmic Impact Assessment			

Domain 2

Cloud Data Security



Cloud Data Lifecycle

Phases

Data Roles

Controlling
Access

Create

Store

Use

Share

Archive

Destroy

Owner / controller

Processor

Custodian

Steward

Subject

Actors

Functions

Locations

Classification

Possible

Allowed

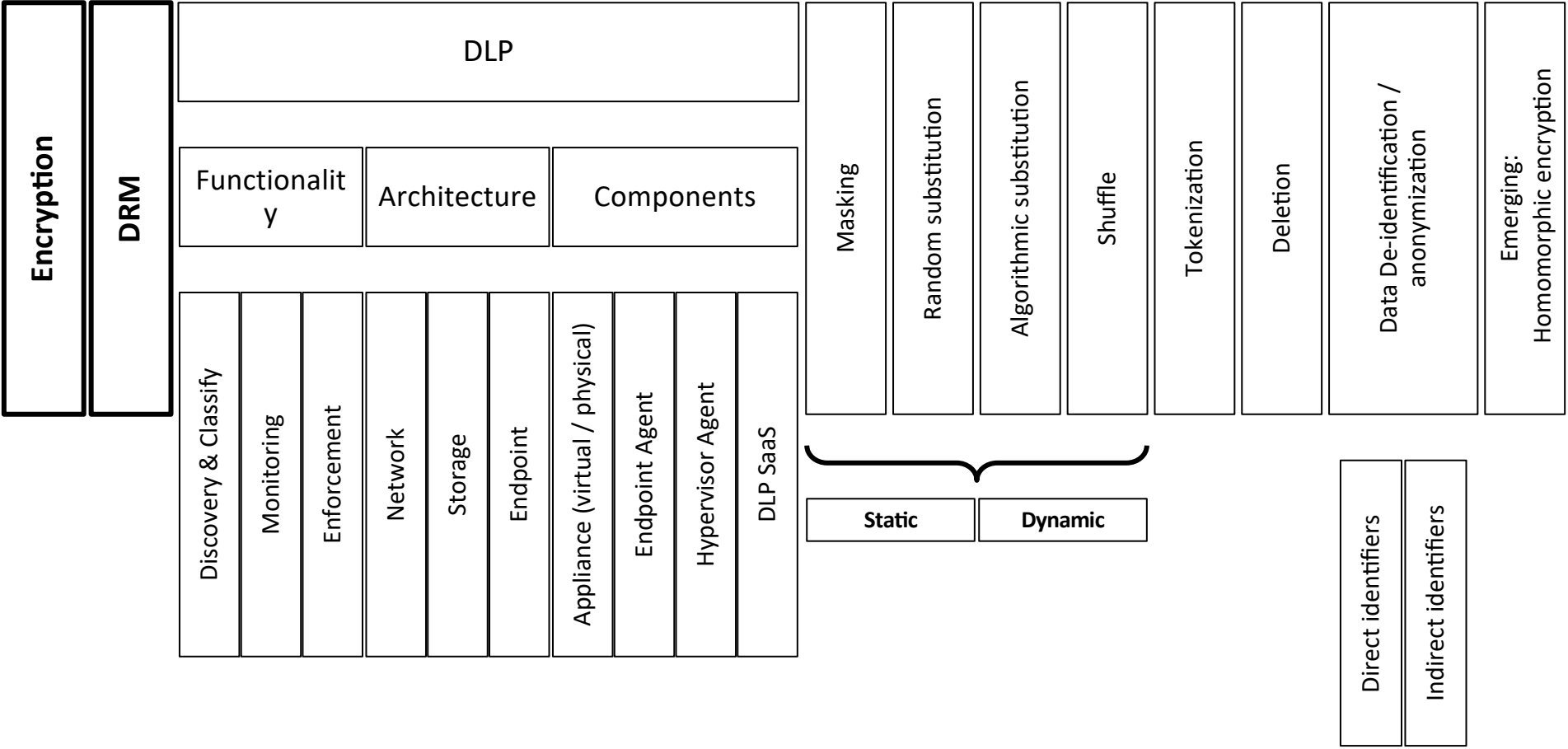
Cloud Data Storage

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



Data Discovery

Types of data

Structured

Unstructured

Metadata

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

Aggregation

Normalization

Correlation

Secure
Storage

Analysis

Reporting

Errors

Modification

Breaches

Digital Rights Management (DRM)

Consumer DRM

Enterprise DRM

Cloud DRM Challenges

Information Rights Management (IRM)

Auditing of access /
use

Signing / sealing

Rights based on
classification

Controlling copy &
pasting, screenshots

Data Retention, Archiving & Deletion

Data retention
policies

Migration to
slower storage

Defensible Destruction

Destruction

Purging

Clearing

Media
Destruction

Shred /
Disintegrate /
Drill

Degauss

Crypto
shredding

Overwrite /
Wipe / Erasure

Format

AI/ML Data Protection

Trustworthy AI starts with secure data, privacy protection, and responsible oversight.

Dataset and Model Privacy					Dataset and Model Security									
Privacy-Preserving Techniques			Privacy Threats		Dual Attack Surface		Build-Time Controls		Pre-Deployment Assurance	Runtime Controls				
Differential Privacy	Federated Learning	Data Minimization	Model Inversion	Data Leakage	Training Data	Model Artifacts	Supply Chain Security	Model Integrity and Signing	Adversarial Robustness Testing	Access Controls	Incident Response	Continuous Model Monitoring		
Privacy-accuracy Trade-off					Model Drift	Metrics								
												Prediction Confidence Distribution		
												Error Rate		
												FP Rate		
												FN Rate		

Domain 3

Cloud Platform and Infrastructure Security



Cloud Infrastructure Components

Major cloud components

Compute

Network

Storage

Virtualization

Management Plane

Virtual Machines

Containers

Serverless Computing

Dedicated
Isolated Networks

Networking Models

Virtual Networks

Cloud Data Storage

Abstraction

Hypervisors

Containerization
Engine

Immutable workloads

Service

Storage

Management

Non-converged

Converged

VLAN

SDN

Type 1: Hardware

Type 2: Operating
System

Infrastructure as Code (IaC)

Management Plane

Single most significant difference	Capabilities										Access			
	Scheduling	Orchestration	Maintenance	Service Catalog	Self-Provisioning	Identity and Access Management	Management APIs	Configuration Management	Key Management & Encryption	Financial Tracking & Reporting	Service / Helpdesk	Web console	APIs	SDKs & CLIs

Data Center Design

[illegible]

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

VM Sprawl

Sensitive data within a VM

Dormant VMs

Instant-on gaps

Resource exhaustion

Hypervisor security

Data comingling

Inter-VM communication (blindspots)

Specific to Cloud

Physical Security

Safety of people

Security Survey

Categories of Controls

Layered Defense

Deter
Delay
Detect
Assess
Respond

Perimeter

Doors / Mantraps

Infrastructure

NFPA

Fire Detection

Fire Suppression

Landscape

Grading

Network

Power

HVAC

Flame

Smoke

Heat

Water

Gas

UPS

Generator

Wet
Dry
Pre-action
Deluge

INERGEN
Argonite
FM-200
Aero-K

Network Defense

Defense in Depth

Zero Trust

Firewalls

Inspection

Endpoint Security

Types

IDS

IPS

IDS/IPS Location

IDS / IPS Detection Methods

Honeypots &
honeynets

Ingress vs. Egress

Packet Filtering

Stateful Packet
Filtering

Application

Firewalls
in the Cloud

Virtual

Physical

Microsegmentation

Geofencing

Host Based

Network Based

Placement in the
Cloud

Pattern

Anomaly

White & Black
Lists

Sandbox

Signature analysis

Stateful matching

Statistical

Protocol

Traffic

Business Continuity Management (BCM)

Business
Impact
Assessment

Measurements
of Time

Types of Plans

Cloud Recovery

Architect
for failure

Chaos
Engineering

Vendor
Lock-in

RPO

RTO

WRT

MTD

Business
Continuity
Plan (BCP)

Disaster
Recovery
Plan (DRP)

Recovery to
Cloud

Recovery
within same
CSP

Recovery to
alternate
CSP

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

Higher baseline security

Responsiveness

Isolated environments

Micro-service architectures

Elasticity

DevOps

Unified management interface

Immutable infrastructure

Limited logging visibility

Increased application scope

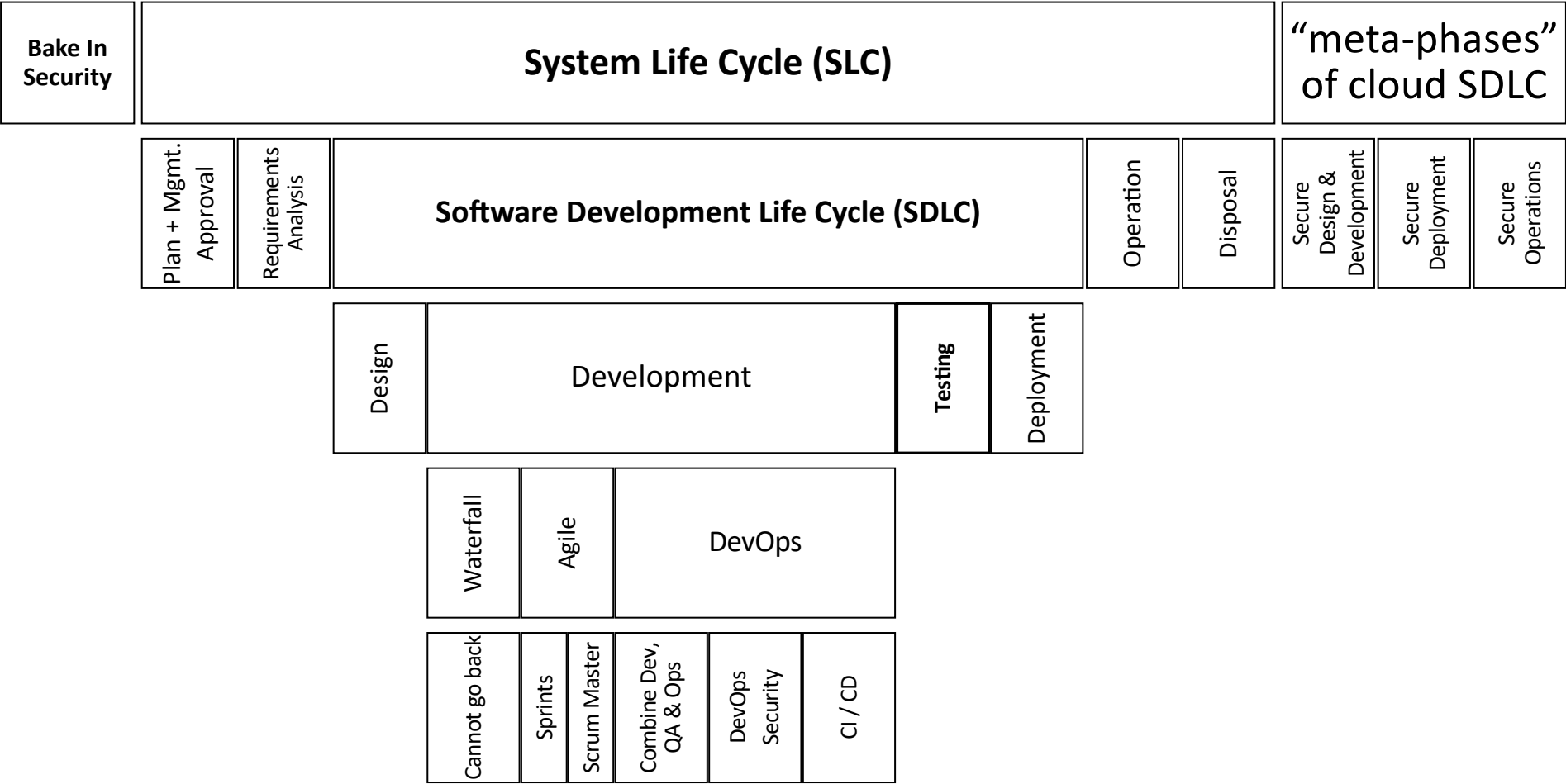
Changing threat models

Reduced transparency

Opportunities

Challenges

Secure Software Development



Security Assessment and Testing

Validation	Software Testing Techniques																			
Verification																				
Rigor based on Value																				
Methods & Tools		Runtime			Access to Code		Software Composition Analysis (SCA)	Vulnerabilities												
Manual	Automated	Static (SAST)	Dynamic (DAST)	Fuzz	Interactive (IAST)	White	Black	Vulnerability Assessment	Penetration Test	Process		Testing Techniques			Types of Scans	Banner grabbing & Fingerprinting	Interpreting & understanding results	False positive vs. False negative		
								Reconnaissance	Enumeration	Vulnerability Analysis	Execution	Document Findings	Perspective	Approach	Knowledge	Credentialed / Authenticated	Uncredentialed / Unauthenticated	CVE	CVSS	
								Internal	External	Blind	Double-blind	Zero (black)	Partial (gray)	Full (white)						

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

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

Proxies

WAF	DAM	FAM	API Gateway
-----	-----	-----	-------------

Access Control

Access Control Principles			Entity	Access Controls Services					Allows users to access multiple systems with a single set of credentials				Privileged User Management	Secrets Management	CASB
Separation of Duties	Need to Know	Least Privilege	Identity	Identification	Authentication				Authorization	Accountability	Single Sign-on Access systems only within the same organization	Federated Access Access systems across multiple entities			
			Identifier	Attributes	Knowledge	Ownership	Characteristic	Single / Multifactor	Kerberos	Trust Relationship	SAML	WS-Federation OpenID OAuth			
Principal / User	Identity Provider	Relying Party / Service Provider	Tokens	Assertions written in XML											

Domain 5

Cloud Security Operations



Cloud Operations

KVM		Access		Hardware Configuration		Hardening		Availability		Monitoring & Control				Distributed Resource Sharing		Backup and Restore																				
Console		Remote	BIOS		Baseline		Clustering		Redundancy		VM		Performance		Network		Application		Hardware		Reservations		Limits		Shares		Dynamic Optimization		OS & VM Config.		Agent-based		Agentless		Snapshots	
SSH			TPM & HSM																																	
RDP																																				

IT Service Management

Strategy

Design

Transition

Operation

Continual
Improvement

Availability

Capacity

Continuity

Service Level

Change

Configuration

Release &
Deployment

Patching

Incident
Management

Problem
Management

Continual
Service
Improvement

Contract

SLA, PLA, & OLA

Negotiable

Non-
negotiable

Click-wrap
Agreements

Patch levels

Deploying

Considerations

Agent

Agentless

Passive

Manual

Automated

Time zones

Instant-on
gaps

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

Applicable Law

Jurisdiction

Data Privacy
Acts

Conflicting
international
legislation

OECD Guidelines

Cross-border
Data Transfers

Roles

Regulated PII

Contractual PII

GDPR

GAPP

Collection
Limitation

Data Quality

Purpose
Specification

Use Limitation

Security
Safeguards

Openness

Individual
Participation

Accountability

Data Subject

Data Owner /
Controller

Data
Custodian

Data
Steward

Data
Processor

Outsourcing & Cloud Contracts

Assess
Provider Risks

Accountability vs.
Responsibility

Contracts / Agreements

Cloud Audit

Contract
Management

Vendor
Management

Supply Chain
Management

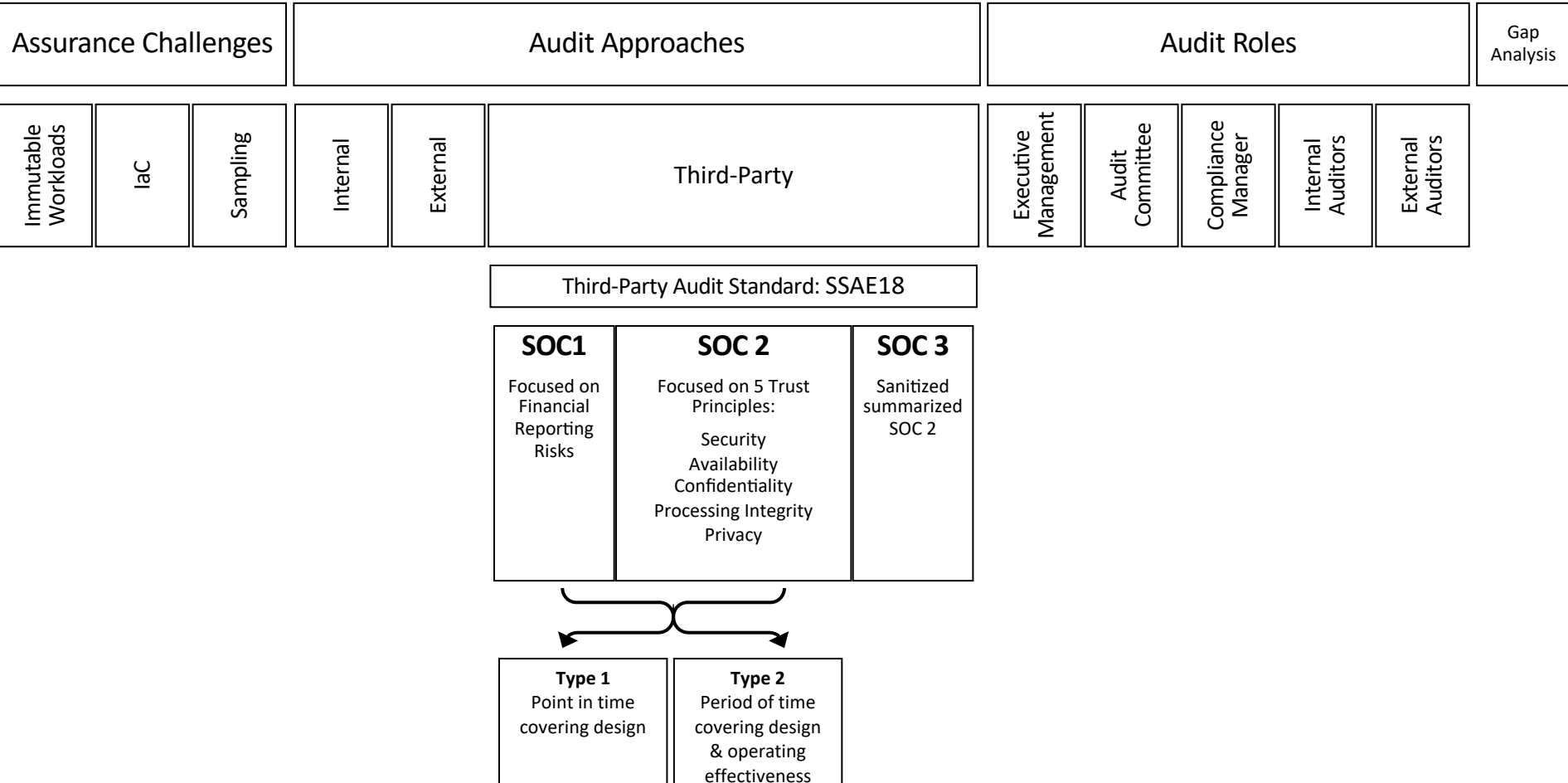
MSA

SOW

SLA

NDA

Cloud Audit

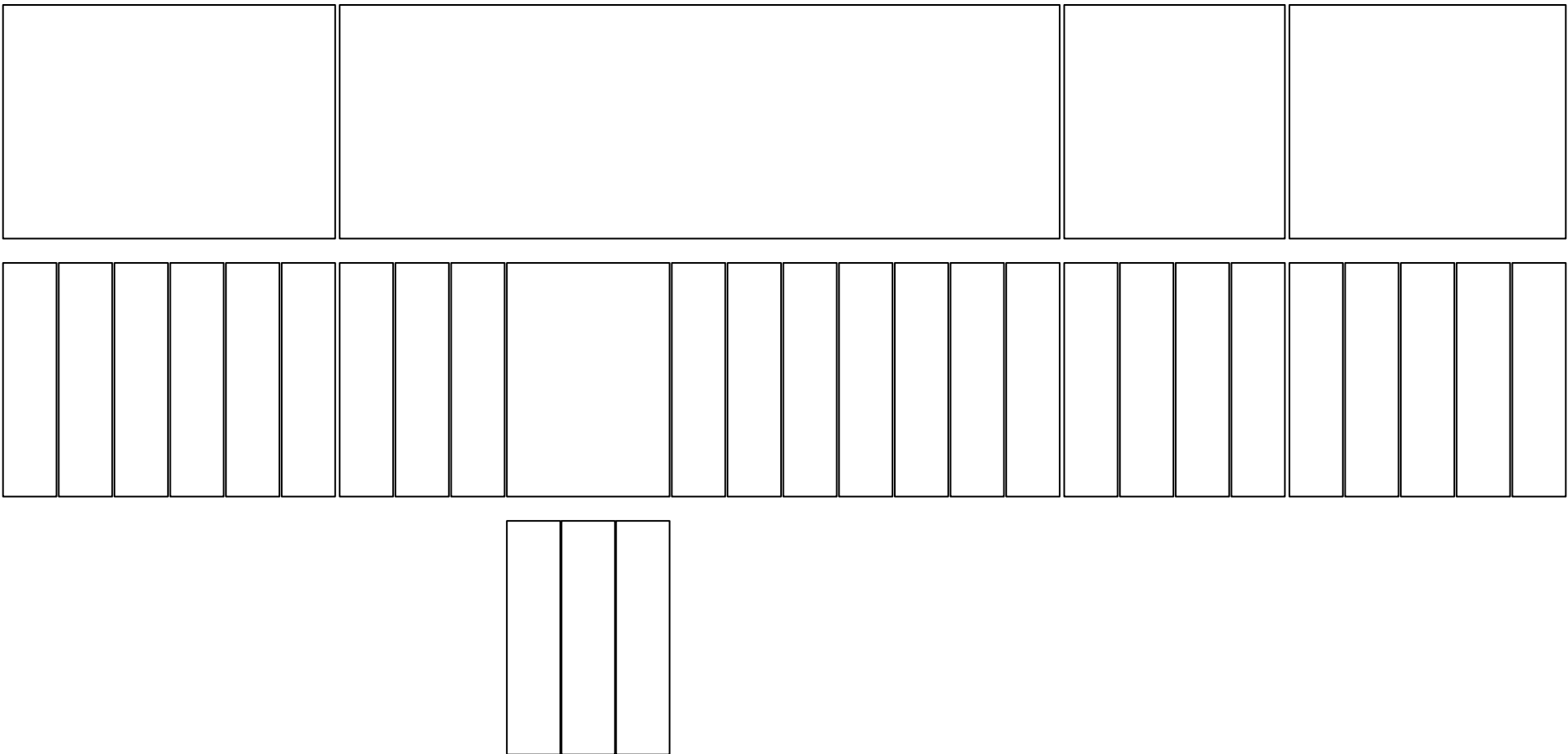


Printable Blank CCSP MindMaps

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

Print pages **40** to **70**

Cloud Computing

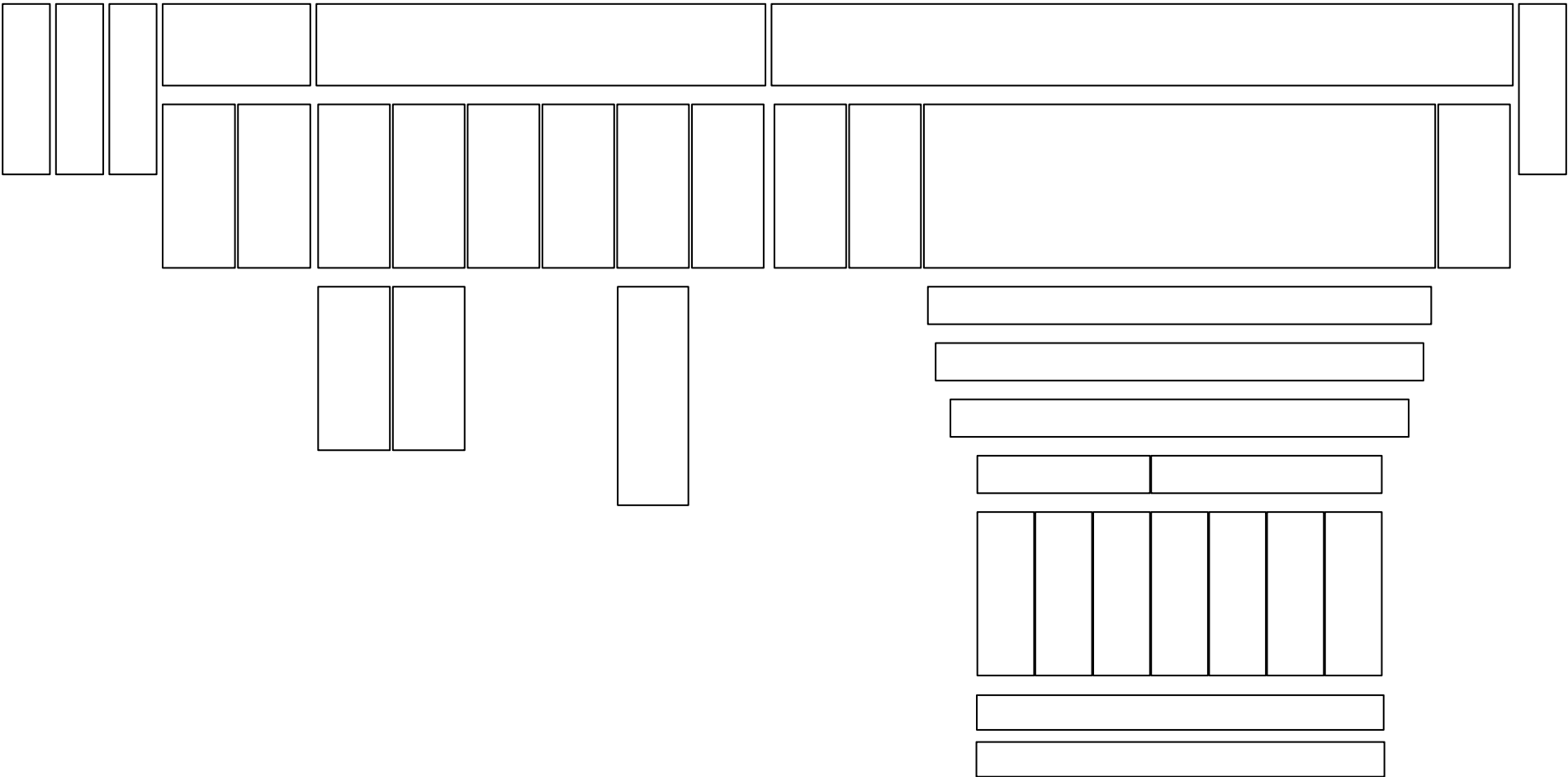


Alignment of Security Function to Business Strategy

--

--

Risk Management



Cost Benefit Analysis

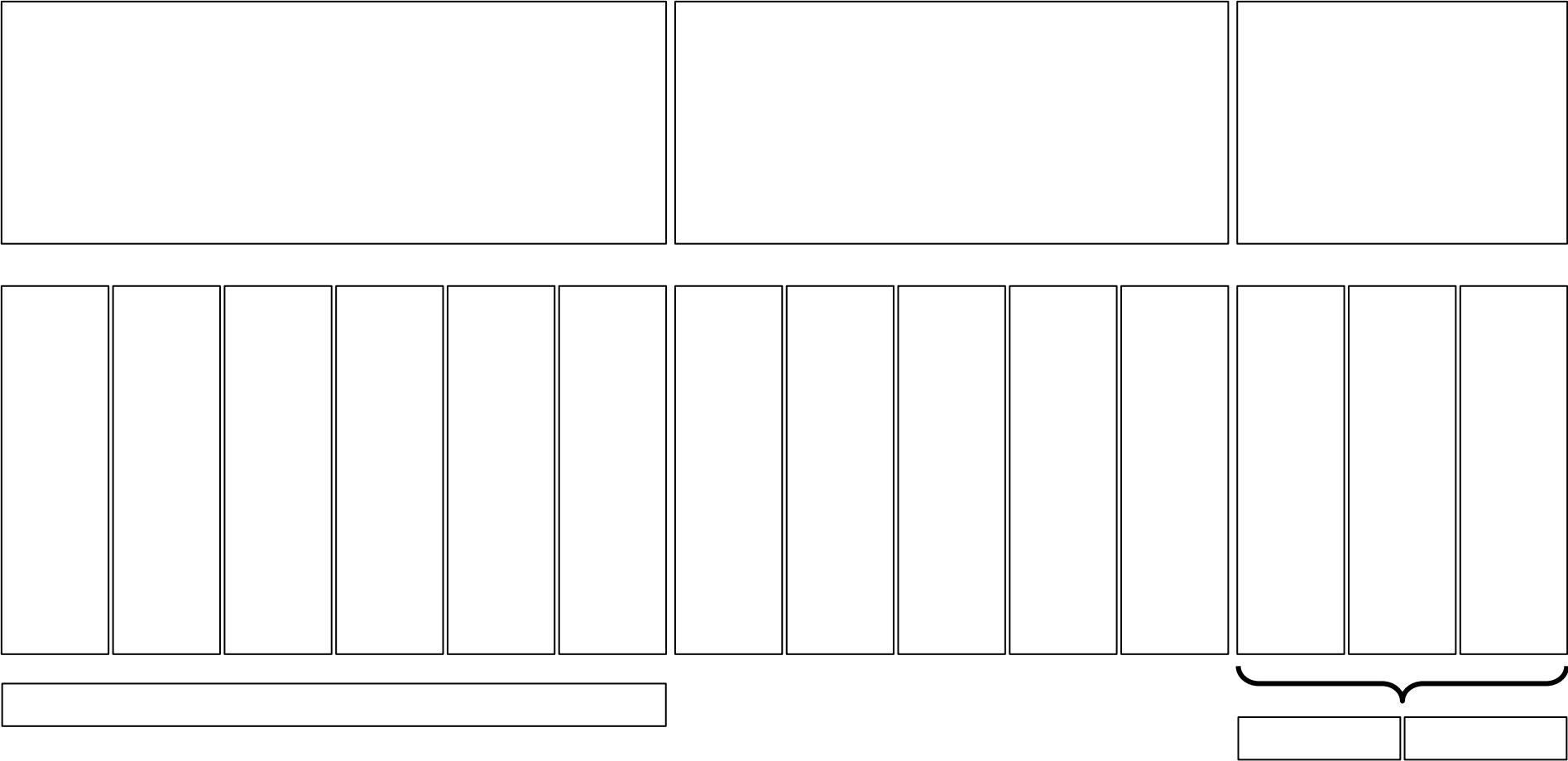
--	--	--	--	--	--	--	--

Evaluation Criteria

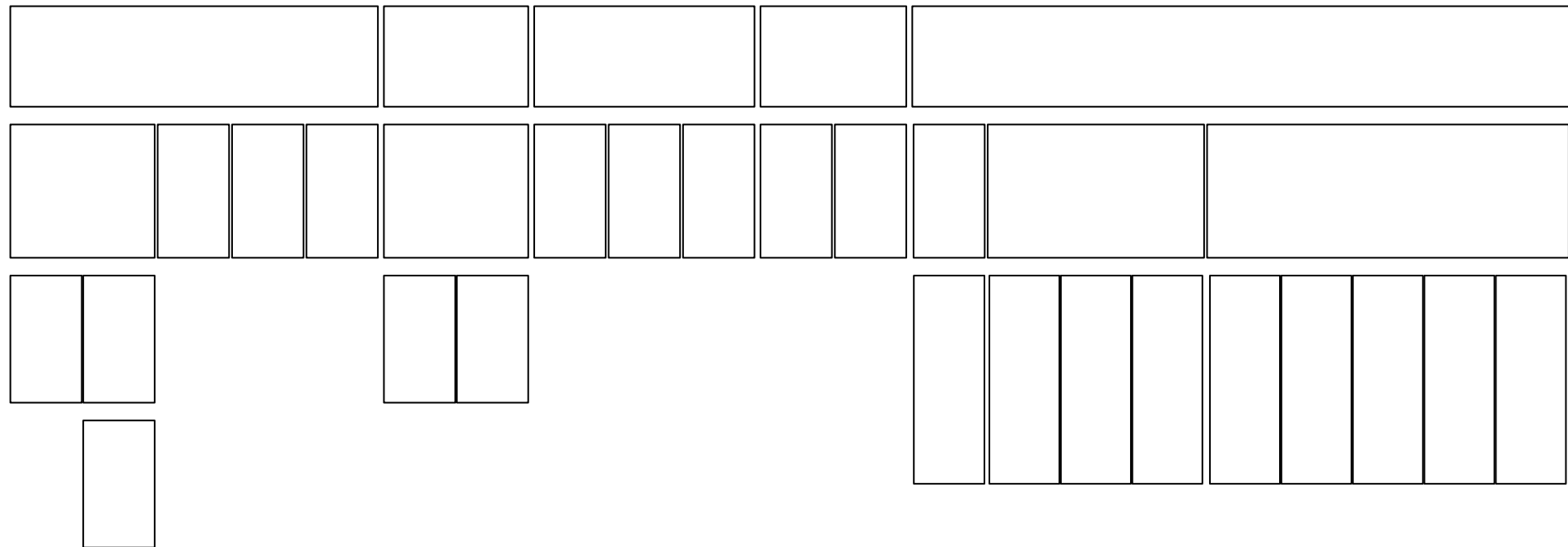
AI/ML Foundations, Risks, and Governance

[illegible]

Cloud Data Lifecycle



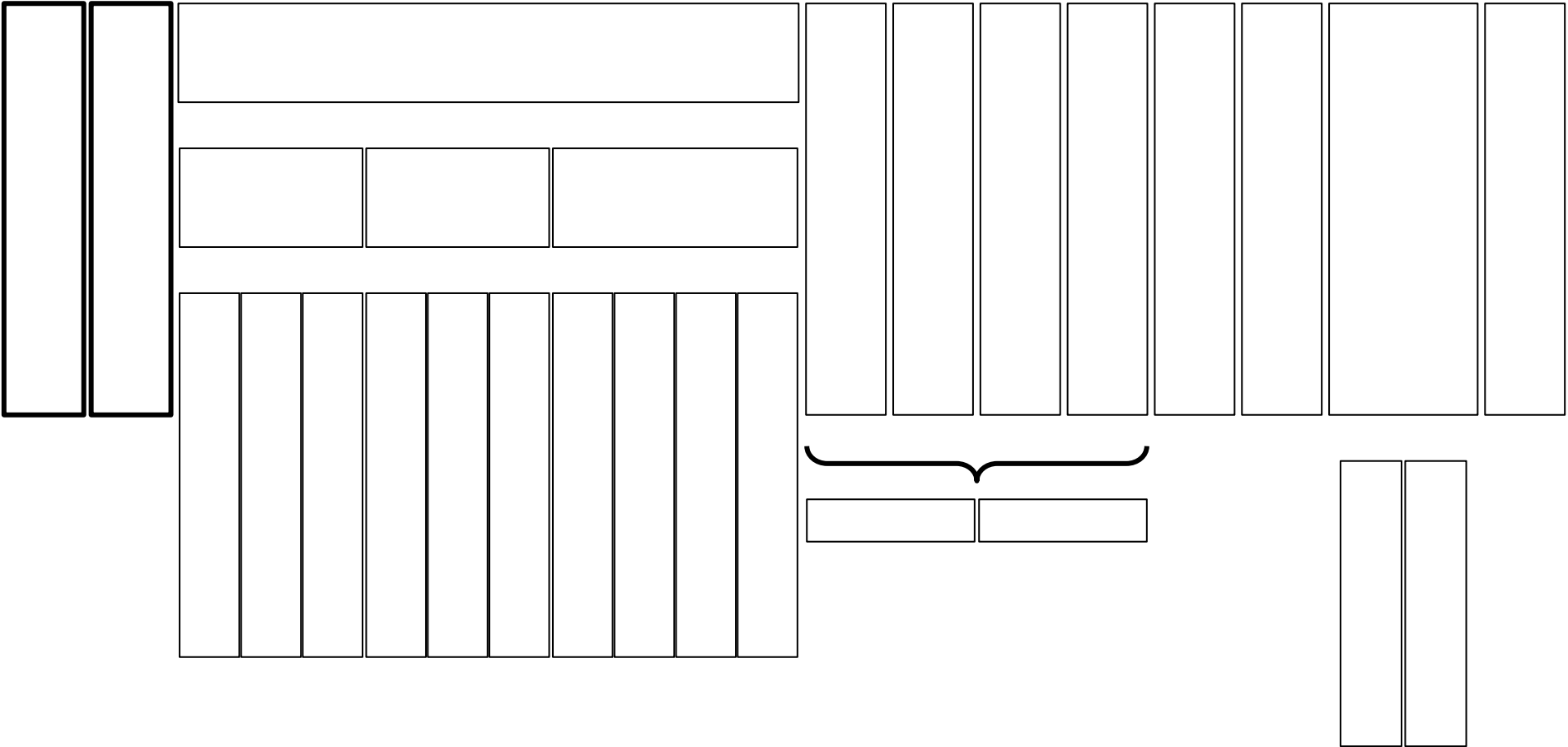
Cloud Data Storage



Threats to Storage



Data Security Strategies



Digital Rights Management (DRM)

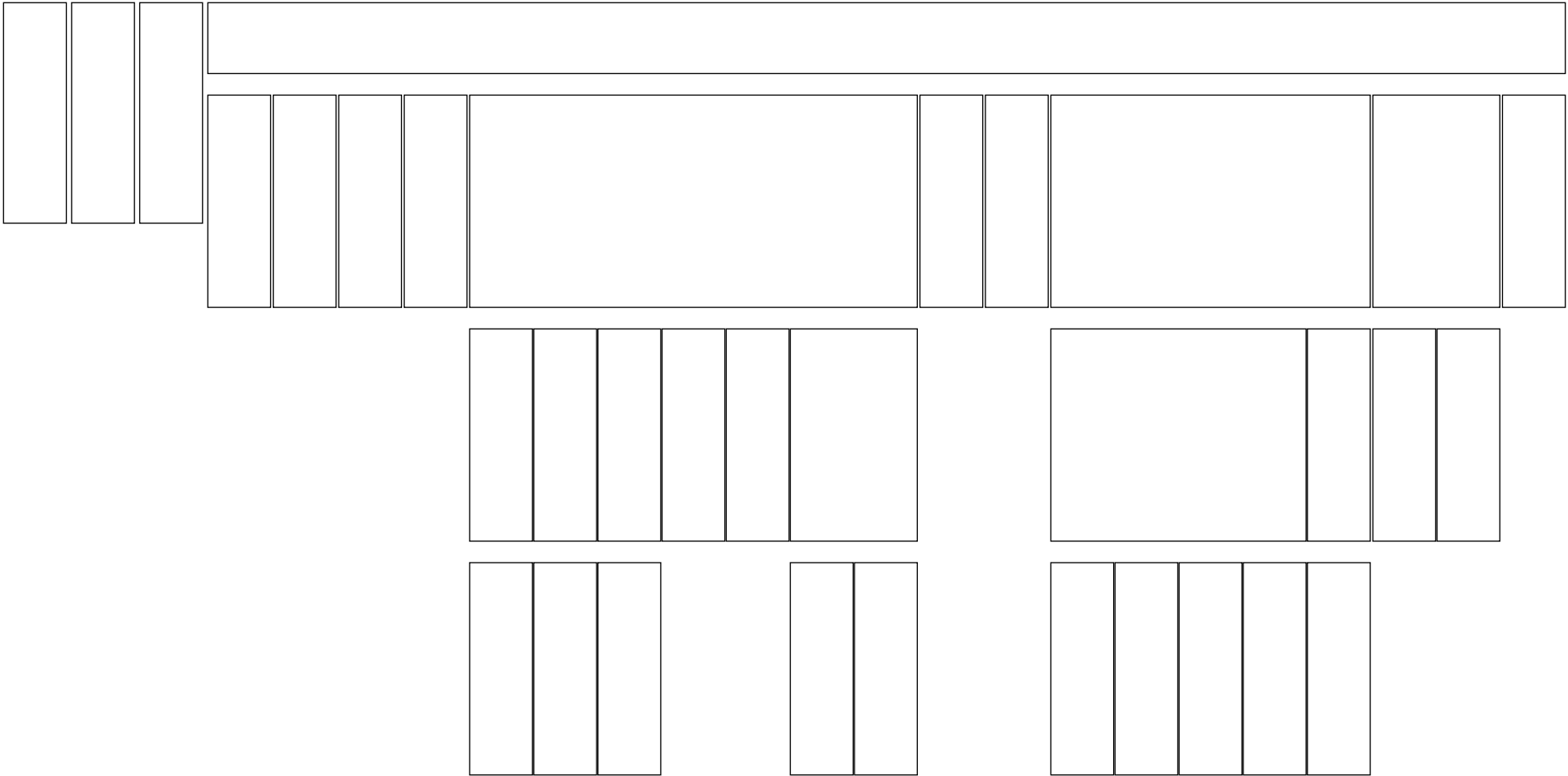
Data Retention, Archiving & Deletion

AI/ML Data Protection

Management Plane

[illegible]

Data Center Design



Physical Security

--

--	--	--

--	--	--	--	--	--	--

--	--	--	--	--	--	--	--	--

--	--

--	--

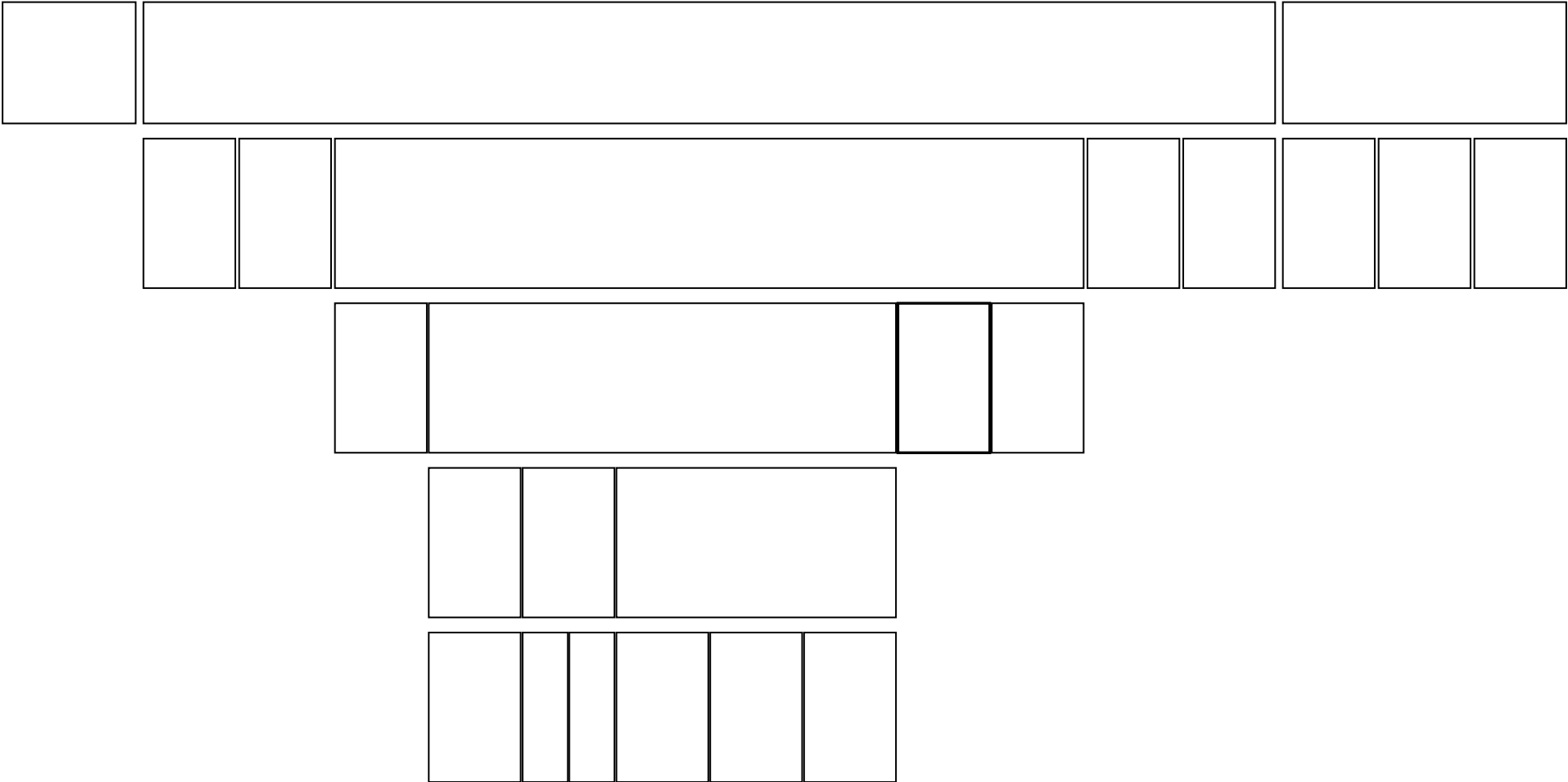
Business Continuity Management (BCM)



Cloud Development

[illegible]

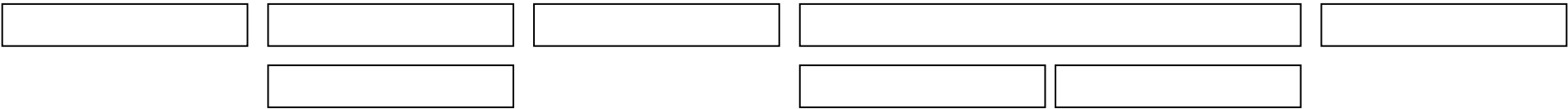
Secure Software Development



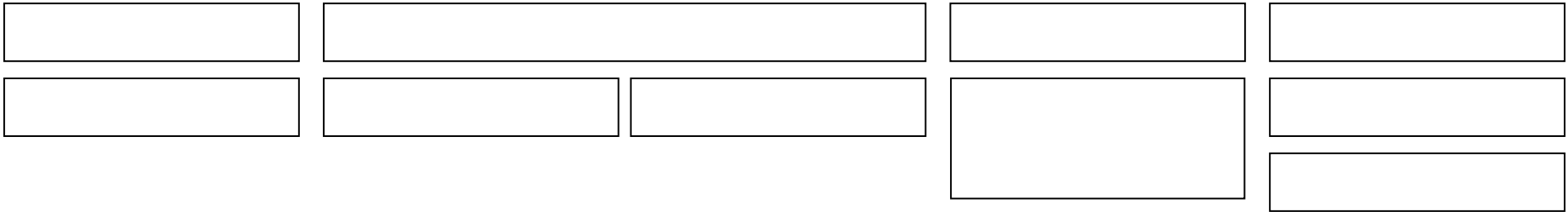
Common Vulnerabilities & Threat Modeling

Verified Secure Software

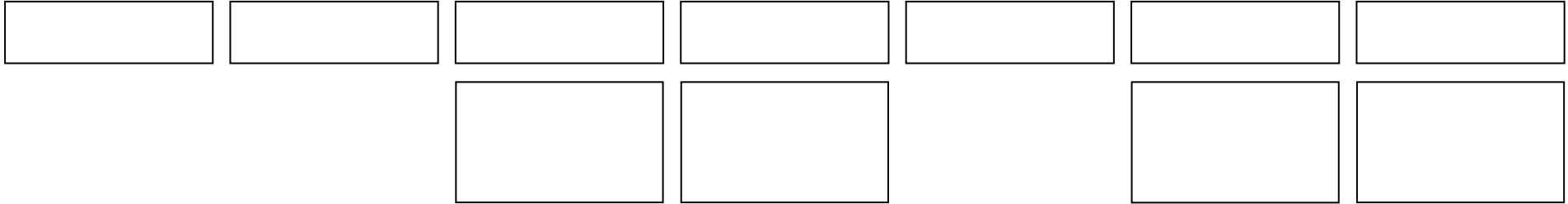
Cryptographic Services



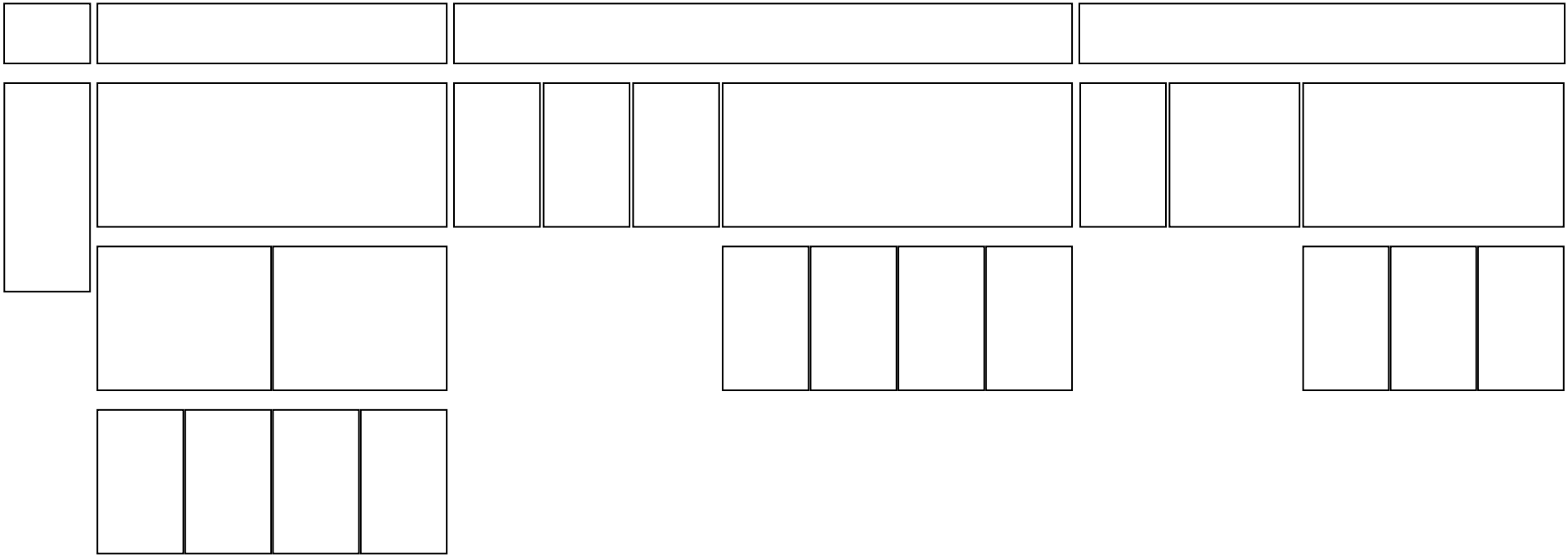
Cryptography



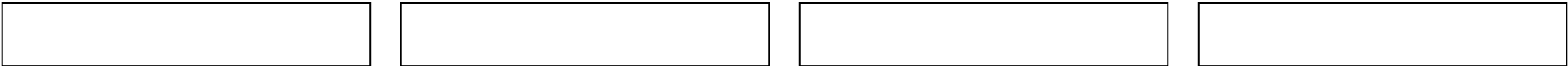
Key Management



Crypto in the Clouds



Proxies



Access Control

The diagram illustrates a hierarchical tree structure of rectangles. The root is a large rectangle at the top, which branches into three smaller rectangles. These further branch into more rectangles, creating a complex, non-linear layout. The rectangles are white with black outlines, and the branching pattern suggests a recursive or fractal-like construction.

Cloud Operations

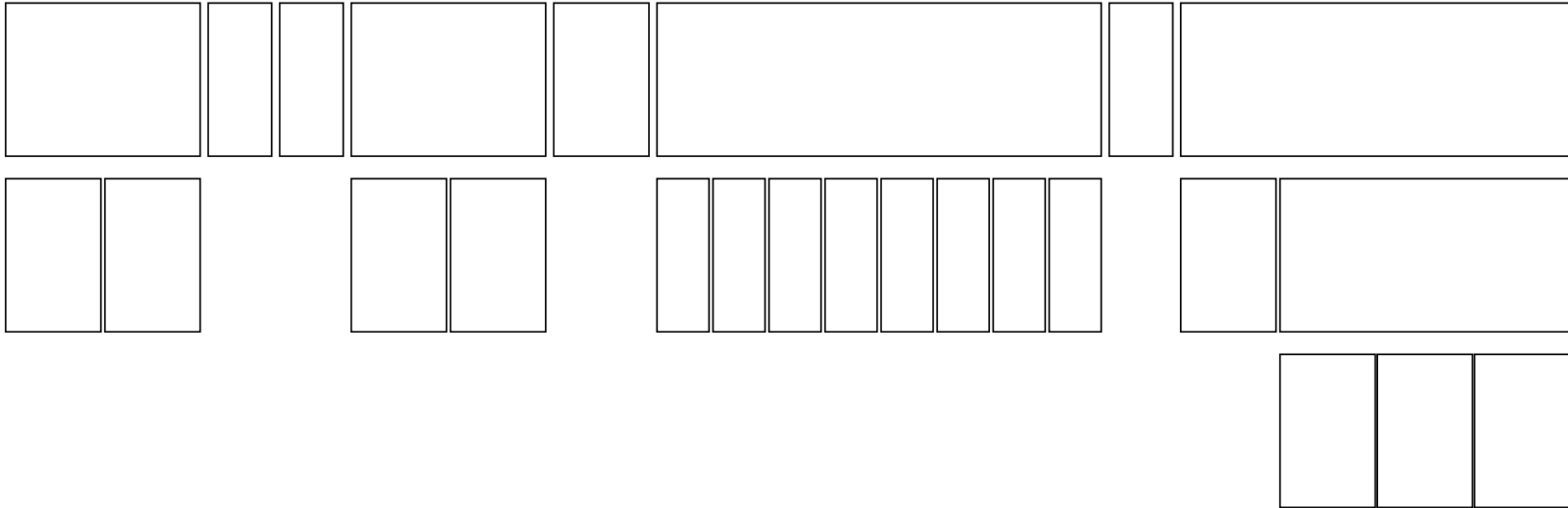
--	--	--	--	--	--	--	--

[illegible]

--	--	--	--

--	--	--	--	--	--	--

Privacy



Outsourcing & Cloud Contracts



Cloud Audit

